

Diritto e Nuove Tecnologie

saggi di informatica giuridica avanzata



a cura dell'associazione D-Lex

Diritto e Nuove Tecnologie

saggi di informatica giuridica avanzata

Prefazione a cura della Prof.^{ssa} Avv. Irene Sigismondi



a cura dell'associazione D-Lex © 2007

Scientia et potentia humana in idem coincidunt.
Francis Bacon, « de dignitate et augmentis scientiarum », 1623

*I computer sono incredibilmente veloci, accurati e stupidi.
Gli uomini sono incredibilmente lenti, inaccurati e intelligenti.
Insieme sono una potenza che supera l'immaginazione.*
Albert Einstein, 1954

TUTTE LE COPIE DEVONO RECARE IL CONTRASSEGNO DELLA S.I.A.E.

www.d-lex.org

info@d-lex.org

Progetto editoriale ed organizzazione tecnica a cura di Sandro Carboni e Vincenzo Russo /
Associazione Professionale CRR Legal

ISBN
© 2008

Prima edizione: 2008

Ogni responsabilità per il contenuto dei singoli scritti appartiene al rispettivo autore.

INDICE

Presentazione della Prof. ^{ssa} Avv. Irene Sigismondi	pag. 13
Prefazione	pag. 15

PARTE PRIMA

Il diritto dell'informatica tra teoria e pratica

CAPITOLO I pag. 18

L'EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO (Avv. Giovanni Amoruso)

1. Premessa. La disciplina normativa del documento informatico e della firma digitale nel D.P.R. 513/1997
2. Il documento informatico: nozione, requisiti e disciplina giuridica.
3. La firma digitale.
4. Valore ed efficacia probatoria del documento informatico nel d.P.R. 445/2000.
5. Valore ed efficacia probatoria del documento informatico nel d.lgs. 82/2005 (c.d. C. A. D.) e relative modifiche.

CAPITOLO II pag. 30

L'UTILIZZO DEL SOFTWARE OPEN SOURCE NELLA P.A. (dott. Fabien Desio Presutti)

1. Introduzione.
2. Open source e Free software, definizioni e differenze.
3. Open Source e diritto d'autore.
4. Le licenze di software libero, la GPL.
5. Open source e P.A. - Quadro storico di riferimento.
6. La direttiva sull'Open Source.
7. L'Osservatorio Open source presso il CNIPA.
8. La situazione nelle P.A.L.
9. I vantaggi per la P.A.
10. La questione economica - Il Value Management.
11. La situazione e le iniziative in Europa.
12. La direttiva sull'Open Source in Francia.
13. La direttiva sull'Open Source in Germania.
14. Formati aperti e formati standard.
15. Il formato Open Document Format (ODF).

16. Il caso Open Office.org
17. L'espansione di ODF e Open Office.org.
18. Considerazioni conclusive.

CAPITOLO III

pag. 54

INTEGRAZIONE DI BANCHE DI DATI IN AMBIENTE SOCIO-SANITARIO (dott. Roberto Perdicaro)

1. Premessa.
2. Open source e Free software, definizioni e differenze.
3. Open Source e diritto d'autore.
4. Le licenze di software libero, la GPL.
5. Open source e P.A. - Quadro storico di riferimento.
6. La direttiva sull'Open Source.
7. L'Osservatorio Open source presso il CNIPA.
8. La situazione nelle P.A.L.
9. I vantaggi per la P.A.
10. La questione economica - Il Value Management.
11. La situazione e le iniziative in Europa.
12. La direttiva sull'Open Source in Francia.
13. La direttiva sull'Open Source in Germania.
14. Formati aperti e formati standard.
15. Il formato Open Document Format (ODF).
16. Il caso Open Office.org.
17. L'espansione di ODF e Open Office.org.
18. Considerazioni conclusive.

CAPITOLO IV

pag. 85

GLI ATTI AMMINISTRATIVI ELETTRONICI TRA DISCREZIONALITÀ E VINCOLATIVITÀ (Avv. Vincenzo Russo)

1. Considerazioni introduttive.
2. Le diverse accezioni di atto amministrativo elettronico.
3. I principali problemi del dell'atto amministrativo ad elaborazione elettronica.
4. L'atto amministrativo elettronico discrezionale: appunti per una ricostruzione.
5. l'atto amministrativo elettronico discrezionale e i sistemi esperti: uno sguardo al futuro.

PARTE II

Il diritto dell'informatica tra l'accesso e la tutela dei dati personali

CAPITOLO V

pag. 101

IL DIRITTO DI ACCESSO AI DOCUMENTI DELLA P.A., IN RELAZIONE ALLA LEGGE 675/96 SULLA PRIVACY E AL DIRITTO ALLA RISERVATEZZA (dott.ssa Imma Barbato)

1. La legge 31.12.1996 n. 675 sulla privacy e l'accesso alla documentazione della pubblica amministrazione.
2. Il trattamento dei dati personali della P.A. e il diritto di accesso di cui alla legge 241/90.
3. L'art. 27 della legge 675/96.
4. Le responsabilità penali.
5. I rapporti tra riservatezza ed accesso alla luce della normativa in tema di tutela dei dati personali.
6. Il diritto di accesso dopo la legge 15/2005.
7. Rapporti tra diritto di accesso e tutela della riservatezza.
8. Conclusioni.

CAPITOLO VI

pag. 113

LA TUTELA DEI DATI PERSONALI NELLE ATTIVITÀ PRODUTTIVE (Avv. Giuliana Astarita)

1. Premessa.
2. Il diritto alla tutela dei dati personali e l'attività d'impresa.
 - 2.1. La firma digitale.
 - 2.2. La tutela dei dati personali nel rapporto di lavoro.
 - 2.3. La tutela dei dati personali e la concorrenza.
 - 2.4. La tutela dei dati personali ed il rapporto con i consumatori e gli utenti. L'attività di *marketing* e lo *spamming*.
3. I costi della tutela dei dati personali.
4. La tutela dei dati personali come qualità e risorsa aziendale.
5. conclusioni.

CAPITOLO VII

pag. 128

L'ANALISI DEI RISCHI NEL D.P.S. DEGLI EE.LL.:LE RESPONSABILITÀ ASCRIVIBILI AL DIPENDENTE (dott.ssa Laura Pea)

1. Premessa.
2. La normativa in materia di sicurezza informatica.
3. Il concetto di sicurezza.
4. La normativa in materia di sicurezza informatica.
5. La sicurezza informatica negli anni '90.
6. Il boom di internet.
7. La sicurezza informatica negli anni 2000.
8. I dati dell'Osservatorio sulla sicurezza e Criminalità ICT (OCI).
9. Il trattamento dei dati.
10. Lo standard ISO/IEC17799:2000.

11. Il trattamento dei dati negli EE.LL.
12. L'analisi dei rischi.
13. I Comportamenti degli operatori.
14. Gli Insider.
15. Eventi relativi agli strumenti.
16. Eventi relativi al contesto.
17. Le responsabilità del dipendente.
18. Pronunce giurisprudenziali.
19. Conclusioni.

CAPITOLO VIII

pag. 145

LE INTERCETTAZIONI: IMPLICAZIONI PER GLI OPERATORI DI TELEFONIA MOBILE
(dott.ssa Rina Lancellotti)

1. Considerazioni introduttive.
2. Delle intercettazioni in generale: definizione e profili di legittimità.
3. Intercettazioni telefoniche e prestazioni obbligatorie.
4. Conclusioni.

CAPITOLO IX

pag. 159

PHISHING & E-BANKING (dott. Sandro Carboni)

1. Phishing: “pescare informazioni private”.
2. Unico disegno criminoso.
3. E-Banking.
4. Analisi, dati, previsioni.

CAPITOLO X

pag. 171

ASPETTI LEGALI PER LA PUBBLICAZIONI DI SITI E-COMMERCE E CASI STUDIO
(dott. Danilo Bacci)

1. Considerazioni introduttive e definizioni.
 - 1.1. Condizioni e presupposti amministrativi per l'avvio dell'attività di commercio elettronico.
 - 1.2. Sanzioni e partita IVA nel sito web.
 - 1.3. Disciplina del commercio elettronico.
 - 1.4. Contratto concluso dai consumatori e Codice del Consumo.
 - 1.5. Disposizioni sulla riservatezza e Codice della Privacy.
2. Autodisciplina e conciliazione on line.
3. Casi studio.

CAPITOLO XI

pag. 204

LA TUTELA DEL NOME A DOMINIO (Avv. Luca Ismaele Lodrini)

1. Considerazioni introduttive.
2. Natura giuridica.
3. Rapporti con il marchio.
4. Tutela stragiudiziale.
5. L'arbitrato irrituale.
6. La procedura di riassegnazione.
7. Tutela giudiziale.

CAPITOLO XII

pag. 213

LA CONSERVAZIONE DELLE SCRITTURE CONTABILI IN FORMATO DIGITALE
(Dott.ssa Maria Maniccia)

1. Considerazioni introduttive.
2. Archiviazione e conservazione in ambiente digitale.
3. Il processo di conservazione sostitutiva: oggetto e finalità.
4. Documenti informatici, documenti analogici unici e non unici.
5. La conservazione sostitutiva dei documenti informatici rilevanti ai fini tributari.
6. I documenti informatici rilevanti ai fini tributari – ambito di applicazione del Decreto ministeriale 23 gennaio 2004.
7. Le caratteristiche dei documenti informatici rilevanti ai fini tributari: formazione emissione, esibizione e memorizzazione.
8. Il processo di conservazione dei documenti informatici rilevanti ai fini tributari.
9. Il riversamento e l'esibizione dei documenti informatici rilevanti ai fini tributari.
10. La tenuta e la conservazione sostitutiva delle scritture contabili.
11. Tenuta delle scritture contabili con modalità informatiche.
12. conservazione delle scritture contabili con modalità informatiche.
13. Conservazione sostitutiva di scritture contabili stampate su supporto cartaceo.
14. Invio dell'impronta all'Amministrazione finanziaria.
15. Esempi di procedimenti di conservazione di scritture contabili.
16. Il responsabile della conservazione.
17. L'intervento del pubblico ufficiale.
18. Il manuale della conservazione.
19. I supporti per la conservazione sostitutiva in formato digitale.
20. Conclusioni.

CAPITOLO XIII

pag. 238

INFORMATIZZAZIONE DEL SISTEMA NORMATIVO IN AMBITO PUBBLICO E
IMPATTO DELLE NUOVE TECNOLOGIE SULLA PRODUZIONE NORMATIVA
(dott. Raffaele Montanaro)

1. Introduzione.

2. Il processo di informatizzazione del *corpus* normativo attraverso le disposizioni emanate.
3. Analisi del processo tecnico di informatizzazione degli atti normativi, la rappresentazione informatica del testo normativo: problemi e procedure.
4. L'informatizzazione come occasione per il riordino e la semplificazione del corpus normativo.
5. Conclusioni.
6. Allegato n. 1.
7. Allegato n. 2.

Postfazione a cura dell'associazione D-Lex

pag. 261

BIBLIOGRAFIA DI ORIENTAMENTO

pag. 262

PRESENTAZIONE

La raccolta di saggi che ora vede la luce è il risultato della combinazione e dell'interazione tra formazione avanzata, il *Master in Diritto dell'Informatica e Teoria e Tecnica della Normazione* dell'Università La Sapienza di Roma e dell'applicazione dei contenuti appresi ad ambiti specifici di interesse professionale o scientifico.

Il Master è un percorso formativo che è entrato non da qualche anno nella tradizione italiana, perché appartiene più direttamente all'esperienza di tipo anglosassone, dove accanto alla teoria si cerca di offrire a chi esce dall'Università competenze tecniche, pratiche e professionali con un taglio specialistico: anche questo Master, che giunge alla VII edizione, risponde a questa esigenza, con il vantaggio, nel particolare settore che è l'informatica giuridica ed il diritto dell'informatica, di contribuire alla creazione di quella *community of practice* che ancora manca nel diritto, soprattutto per il grande apporto che può arrivare proprio dai giovani, avvantaggiati nella facilità di leggere nel quotidiano sia il lato teorico delle problematiche, anche nei risvolti applicativi, sia le ripercussioni nel mondo giuridico.

Il pregio dei contributi che qui si presentano è la capacità che ciascuno ha avuto di sintetizzare, con chiarezza e lucidità, i singoli problemi affrontati che spesso hanno una radice antica, ma che oggi producono frutti nuovi, proprio grazie all'innesto delle nuove tecnologie: la sfida è riuscire a capire che la nuova prospettiva che esse impongono rispetto all'analisi degli istituti del diritto richiede la capacità di integrare la tradizionale preparazione del giurista con uno strumentario adeguato.

Nello specifico, i saggi possono essere raccolti in base ai diversi settori tradizionali del diritto, oppure accorpati in base ai problemi che le tecnologie pongono al giurista che si prepara ad affrontarli con successo.

Secondo lo schema tradizionale si va dal **diritto amministrativo** (Imma Barbato, *Il diritto di accesso ai documenti della P.A.*; Raffaele Montanaro, *Informatizzazione del dato normativo in ambito pubblico e impatto delle nuove tecnologie sulla produzione normativa*; Laura Pea, *L'analisi dei rischi nel D.P.S. degli Enti Locali*; Roberto Perdicaro, *Integrazione di banche dati in ambiente socio-sanitario*; Fabien Desio Presutti, *Utilizzo del software Open Source nella P.A.*; Vincenzo Russo, *Atti amministrativi discrezionali*), al **diritto civile e commerciale** (Giovanni Amoroso, *Valore ed efficacia probatoria del documento informatico*; Danilo F. Bacci, *Aspetti legali per la pubblicazione di siti di e-commerce e casi di studio*; Luca Ismaele Lodrini, *La tutela del nome a dominio*, Maria Maniccia, *La conservazione delle scritture contabili in formato digitale*), al **diritto penale** (Sandro Carboni, *Phishing & e-banking*, Rina Lancellotti, *Le intercettazioni: implicazioni per gli operatori di telefonia*).

Con un'altra chiave di lettura, però, che risponde alle sollecitazioni delle nuove tecnologie, si vedono considerati nei vari contributi i **problemi giuridici delle banche dati**, a livello pubblico e privato, il trattamento dei dati personali, per l'esercizio di un'attività commerciale on-line o per l'accesso ai documenti della P.A.,

ma anche per i dati sensibili in ambiente socio-sanitario o in caso di intercettazioni a fini di indagini giudiziarie.

Ancora il ***problema della formazione della volontà nel documento privato e pubblico*** con i risvolti sul valore probatorio e sulla discrezionalità pubblica, ***il problema delle vulnerabilità tecnologiche***, che possono produrre rischi da valutare nei documenti programmatici sulla sicurezza per soggetti privati e pubblici, possono favorire la violazione della proprietà intellettuale dei nomi a dominio o addirittura la commissione di reati nel c.d. *phishing*. Ma ancora si pongono i ***problemi dell'adattamento tecnologico*** spesso legati anche alle c.d. *legacies*, alla rapida obsolescenza delle tecnologie ed alla ricerca dell'interoperabilità, quando occorre pensare al futuro pur conservando la possibilità che ciò che è tecnologicamente accessibile oggi rimanga tale anche in futuro (e qui si pensi alla conservazione delle scritture contabili ed agli sforzi della pubblica amministrazione per incentivare l'utilizzo dell'Open Source software in modo permanente, ma anche con le dovute garanzie di sicurezza e stabilità).

Problemi vecchi e nuovi, come si vede, ciascuno trattato in modo organico e sintetico al tempo stesso, con riferimenti diretti alla legislazione ed alla giurisprudenza, spesso con analisi di casi di studio, ma soprattutto con la visione di un *giurista technology-savvy*, consapevole delle potenzialità e dei rischi che le tecnologie portano nel mondo del diritto.

La lettura di questi contributi è consigliata ai professionisti per rispondere alle problematiche quotidiane che si presentano nella pratica; ai funzionari pubblici per formarsi una base di conoscenza sul mondo che cambia nell'amministrazione e nel privato, che sempre di più dialoga con l'amministrazione stessa anche nel perseguimento di obiettivi condivisi; ai giovani, studenti o studiosi, che cercano uno strumento di riferimento scritto in modo agile e scorrevole, sintetico e completo, su temi che non sono ancora oggetto di studio sistematico al di fuori della stretta cerchia di chi conosce anche come la pratica può modificare la teoria.

Infine la lettura è consigliata anche soltanto ai curiosi che spesso si pongono domande sui problemi legati all'utilizzo delle tecnologie e sui risvolti legali che esse necessariamente determinano.

Roma, settembre 2008

Irene Sigismondi

PREFAZIONE

Il presente volume costituisce un'opera di taglio pratico e storico unica nel suo genere: oltre a fornire un supporto indispensabile per chi, operatore o accademico, ha bisogno di un punto di riferimento concreto per la propria attività di giurista applicato alle nuove tecnologie, costituisce nondimeno un sunto critico dello stato dell'informatica giuridica italiana degli ultimi dieci anni.

Alla prospettiva scientifica, sia di stampo universitario che di carattere operativo, si unisce pertanto una prospettiva storica che da una parte mette in evidenza i tratti salienti dell'argomento così come sono stati elaborati nel nostro ordinamento e dell'altra si proietta verso i probabili sviluppi futuri della disciplina.

Alcune informazioni, alcuni dati e alcune prospettive, pertanto, andranno lette con lo sguardo dello storico e del sociologo del diritto più che del tecnico o dello studioso di diritto positivo, costituendo altresì un prezioso documento sull'evoluzione del diritto applicato alle nuove tecnologie nel nostro paese.

Tutti i saggi mantengono, oltremodo, una freschezza e un'attualità indiscutibile proprio per l'impostazione che si è voluta dare al lavoro, che parte sempre dai fondamenti della disciplina e dell'istituto e si sofferma sulle problematiche essenziali sottese ai diversi argomenti.

A tal proposito si è preferito mantenere gli scritti così come sono stati concepiti dai rispettivi autori piuttosto che procedere ad un aggiornamento che, tra il momento dell'ideazione e la sua pubblicazione, per la nota legge di Moore che colpisce anche l'editoria informatica, avrebbe avuto bisogno a sua volta di una nuova revisione.

Anche per questo, e pur non rinunciando al fascino e alla comodità del supporto cartaceo, il presente volume può essere consultato anche in formato e-book presso il sito www.dlex.org, che costituirà inoltre il luogo dove prelevare gli aggiornamenti e il materiale che via via si aggiungerà, come uno strumentario, all'opera attuale.

Vincenzo Russo
Presidente associazione D-Lex

Sandro Carboni
Vice presidente associazione D-Lex

PARTE PRIMA

Il diritto dell'informatica tra teoria e pratica

CAPITOLO I

GIOVANNI AMOROSO

FIRMA DIGITALE ED EFFICACIA PROBATORIA DEL
DOCUMENTO INFORMATICO

SOMMARIO: 1. Premessa. La disciplina normativa del documento informatico e della firma digitale nel D.P.R. 513/1997 – 2. Il documento informatico: nozione, requisiti e disciplina giuridica. – 3. La firma digitale. – 4. Valore ed efficacia probatoria del documento informatico nel d.P.R. 445/2000. – 5. Valore ed efficacia probatoria del documento informatico nel d.lgs. 82/2005 (c.d. C. A. D.) e relative modifiche.

1. Premessa. La disciplina normativa del documento informatico e della firma digitale nel d.P.R. 513/1997

Per restare alla insuperata definizione carneluttiana di documento - quale “rappresentazione di atti o fatti giuridicamente rilevanti” - va preliminarmente osservato che tale rappresentazione - l’esternazione del fatto o atto - può avere diverse *forme* (modalità di rappresentazione): scritta, orale, attraverso segnali ottici o sonori, ecc.

Una delle forme di più recente invenzione attraverso cui rappresentare atti o fatti rilevanti per il mondo del diritto è la forma *informatica* del documento, cioè la tecnica di rappresentazione delle informazioni basata sulla tecnologia *digitale*: un sistema di codificazione binaria (*binary digit*) dei documenti testuali, delle immagini e dei suoni che ha il suo fondamento tecnico sullo stato *duale* (binario, appunto) della materia (i circuiti) che vengono attraversati dalla corrente elettrica (positivo-negativo, 0-1).

In materia di documento in forma informatica, per così dire “puro e semplice”, si prescinde da qualsivoglia tecnica di sottoscrizione: i documenti informatici rilevano in quanto tali, nella loro oggettività (nel senso di mera rappresentazione, in questa particolare forma, di un atto, dato o fatto); si prescinde dalla provenienza del documento, dall’imputabilità ad un autore, in una parola dall’elemento soggettivo.

Ai fini della presente indagine bisogna prender le mosse dall’art. 15, co. 2, della legge 59/1997 (c.d. Legge Bassanini 1), che ha stabilito il principio generale secondo cui gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con documenti informatici sono validi e rilevanti a tutti gli effetti di legge.

Tale disposizione è di cospicuo interesse, se si tiene conto del fatto che antecedentemente alla sua emanazione soltanto alcune norme, in modo del tutto frammentario, avevano preso in considerazione la rilevanza giuridica del documento informatico.

Per citarne solo alcune, si vedano l'art. 22 della legge sul procedimento amministrativo (legge 241/1990) ovvero le disposizioni contenute nella legge n. 547/1993 che, con riferimento alle fattispecie delittuose della falsità in atti ovvero della rivelazione del contenuto dei documenti segreti, Va, infine, ricordata la disposizione dell'art. 234 c.p.p. che, in tema di prova documentale, consente l'acquisizione di scritti o altri documenti mediante la fotografia, la cinematografia, la fonografia o qualunque altro mezzo.

Il legislatore è giunto alla emanazione di una norma generale sul documento informatico proprio per porre un primo e certo punto di riferimento normativo atto a disciplinare, in via generale, un fenomeno che sempre più prepotentemente stava invadendo anche il mondo del diritto.

Basti pensare al problema della conclusione del contratto per mezzo dello scambio della proposta e della conseguente accettazione tramite e-mail oppure alla possibilità di effettuare la notificazione di un documento mediante posta elettronica.

Si ricorda, inoltre, l'emanazione di un regolamento circa i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici.

Con il recepimento della Direttiva 1999/93/CE e l'emanazione del d.lgs. 10/02 e del d.P.R. 137/2003, il quadro normativo di riferimento ha subito una profonda trasformazione; in particolare, l'articolo 6 del decreto di recepimento ha modificato l'articolo 10 del d.P.R. 445/00, stabilendo che il documento informatico (da intendersi, ai sensi del TU del 2000, come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti e, quindi, non recante alcuna sottoscrizione elettronica), ha l'efficacia probatoria prevista dall'articolo 2712 c.c.

2. Il documento informatico: nozione, requisiti e disciplina giuridica

La definizione contenuta nell'art. 1, co. 1, lett. a) del d.P.R. 513/97 si riferisce esclusivamente al documento informatico in senso stretto e cioè a quello costituito da un insieme di dati in forma digitale, memorizzato su apposito supporto, magnetico o ottico, leggibile esclusivamente mediante un sistema informatico idoneo.

Esulano, pertanto, dalla sfera di applicazione del regolamento di esecuzione dell'art. 15, co. 2, della legge 59/1997 quei documenti che, seppur predisposti attraverso un elaboratore elettronico, sono poi successivamente stampati, per cui diventano direttamente utilizzabili senza più l'imprescindibile ausilio di una macchina (c.d. documento informatico in senso ampio).

Operata questa fondamentale distinzione è stato osservato che la definizione del documento informatico in senso stretto risulta comunque estremamente ampia, in quanto può costituire rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti anche la trasmissione di immagini

memorizzata in un cd rom, la diffusione di suoni ovvero la visualizzazione di grafici planimetrie, ecc.

Si distingue, infatti, all'interno della categoria tra **documento informatico dichiarativo**, che è quello formatosi con il compimento dell'atto dichiarativo reso in forma digitale, e **documento informatico non dichiarativo**.

Perché si possa prender cognizione di un fatto rappresentato da un documento informatico è necessario:

a) che lo stesso non solo venga prodotto in giudizio ma che il Giudice, utilizzando un computer o altro strumento tecnicamente idoneo, compia una apposita attività istruttoria;

b) come è stato chiarito l'utilizzazione di un elaboratore elettronico al fine di ricevere la rappresentazione di fatti da documenti informatici non giustifica il ricorso da parte del Giudice alla consulenza tecnica, trattandosi di una operazione che, oramai, rientra nelle nozioni e nelle capacità dell'uomo medio.

3. La firma digitale

E' opportuno adesso chiarire, seppur brevemente, la nozione di firma digitale, le sue caratteristiche principali e la funzione.

Ancora una volta il ricorso è alla normativa dettagliata contenuta nel d.P.R. 513/97 nonché al d.p.c.m. dell'8 febbraio 1999.

Detta firma è il frutto di un procedimento informatico e crittografico (validazione) per mezzo del quale la si genera e la si appone al documento informatico il quale consente, per mezzo dell'utilizzo di chiavi asimmetriche, una pubblica ed una privata, sia di rendere manifesta una determinata volontà contenuta nel documento stesso da parte di colui che lo sottoscrive, sia di verificarne la provenienza e l'integrità da parte di colui che lo riceve.

Dalla definizione appena data si ricava:

a) che per generare una firma digitale è necessario utilizzare delle chiavi asimmetriche, cioè una coppia di chiavi crittografiche, una pubblica ed una privata, correlate fra loro;

b) che una chiave è detta privata in quanto destinata ad essere conosciuta soltanto dal soggetto titolare; essa consente sia di sottoscrivere il documento informatico (c.d. funzione di autenticazione che da conto della provenienza del documento informatico da un determinato soggetto) sia di leggere (o meglio decifrare) il documento informatico da altri cifrato per mezzo della chiave pubblica (c.d. funzione di segretezza);

c) che per chiave pubblica si intende invece la chiave destinata ad essere resa pubblica, in appositi albi tenuti da soggetti che prendono il nome di Certificatori, ed utilizzabile da parte di chi, destinatario di un determinato documento informatico, intende verificare la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche ovvero da parte

di chi intende render segreto il documento informatico che così potrà essere letto solo ed esclusivamente dal titolare della chiave privata.

In altre parole, se si tiene presente che il sistema delle chiavi asimmetriche presuppone uno stretto collegamento tra la chiave pubblica e quella privata, che rende imprescindibile il loro utilizzo per la cifratura e la conseguente decifratura di un documento informatico, ne segue che l'utilizzo di una o dell'altra o di entrambe riesce a soddisfare diverse esigenze.

In particolare queste sono: 1) **la segretezza**; 2) **l'autenticazione**; 3) **l'integrità del documento informatico**.

La sola segretezza del documento informatico viene perseguita, come sopra già ricordato, cifrando il documento informatico con la chiave pubblica del destinatario. Quest'ultimo, in possesso della chiave privata, sarà l'unico a poter leggere, una volta decifrato il documento informatico, il suo contenuto. Se il documento informatico viene cifrato con la sola chiave privata viene assicurata invece l'esigenza dell'autenticazione o meglio viene sottoscritto così il documento informatico e si garantisce la provenienza dello stesso da un determinato soggetto (cioè dal titolare della chiave privata che non è resa nota ad alcuno).

Se, infine, nello stesso tempo vengono utilizzate sia la chiave privata che la chiave pubblica del destinatario del documento informatico si raggiungerà allo stesso tempo sia lo scopo della segretezza sia quello dell'autenticazione o sottoscrizione del documento stesso.

In ogni caso viene assicurata anche l'integrità del documento informatico. La cifratura dipende, infatti, dal contenuto del documento per cui una sua eventuale alterazione comporterà l'invalidità della procedura informatica di validazione.

4. Valore ed efficacia probatoria del documento informatico nel d.P.R. 445/2000.

Ai sensi dell'art. 1, lett. b, del d.P.R. 445/2000, per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, mentre l'art. 8, comma 1, dispone che il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del medesimo provvedimento.

Con riferimento precipuo alle problematiche probatorie, analizziamo le diverse tipologie di documenti informatici previsti dal d.P.R. 445/2000 e relative modifiche:

a - documento informatico non scritto.

Al documento informatico non sottoscritto è riconosciuta – quanto ai fatti e alle cose rappresentate – l'efficacia probatoria prevista dall'art. 2712 c.c., al pari dunque delle riproduzioni meccaniche (art. 10 co.1 d.P.R. 445/2000 modif.).

In questa ipotesi non si tratta di dimostrare l'imputabilità del documento, essendo privo di sottoscrizione, bensì di stabilire quali siano gli strumenti utilizzati per la formazione di quella rappresentazione informatica spostando il fulcro dell'accertamento giudiziale sul versante dell'attendibilità della riproduzione.

La parte contro cui il documento informatico venga utilizzato avrà l'onere, per evitare la piena efficacia probatoria, di contestare la conformità ai fatti o alle cose rappresentate. Sarà allora la parte che intenda utilizzare la riproduzione informatica a dover assolvere l'onere probatorio a suo carico, anche dimostrando l'inidoneità dello strumento a fornire una corretta rappresentazione della realtà e una sicura riproduzione dei dati.

Anche la Suprema Corte, in varie sue pronunce, ha riaffermato la piena e libera valutazione giudiziale della prova documentale informatica, qualora validamente disconosciuta ai sensi dell'art. 2712 c.c., mentre deve aversi per fatto non contestato in caso di mancato disconoscimento.

Si osserva dunque che nel caso di documento informatico non sottoscritto, l'affidabilità riposta dall'ordinamento appare addirittura maggiore di quanto risulta per un qualunque documento cartaceo non sottoscritto, per il quale non è invocabile, di per sé solo, alcuna efficacia probatoria.

b - documento informatico sottoscritto con firma elettronica.

Il documento informatico sottoscritto con firma elettronica "*soddisfa il requisito legale della forma scritta*" e "*l'obbligo previsto dagli artt. 2214 e seguenti del codice civile*" e che, quanto all'efficacia probatoria, "*è liberamente valutabile dal giudice, tenuto conto delle sue caratteristiche di qualità e sicurezza*"; la normativa indica quindi la rilevanza sostanziale del documento, precisando anche che ad esso "*non può essere negata rilevanza giuridica, né ammissibilità come mezzo di prova*". (art. 10 co. 2 d.P.R. 445/2000).

L'accertamento giudiziale in questione avrà per oggetto sia la provenienza della dichiarazione che il suo contenuto, rimesso quest'ultimo al principio della libera valutazione (art. 116 c.p.c.) e quindi privo della più forte e incontestabile valenza di "piena prova" della scrittura privata riconosciuta e/o autenticata, assegnato alla firma digitale ed elettronica avanzata.

Il documento informatico sottoscritto con firma elettronica rappresenta lo strumento probatorio attualmente più discusso in dottrina; anche perché su questa figura giuridica si innesta l'acceso dibattito dottrinale sul valore probatorio del messaggio e-mail che ha visto protagonista il decreto ingiuntivo n. 848/03 del Tribunale di Cuneo.

L'esibizione di tale documento informatico comporterà l'accertamento giudiziale della sua autenticità e data di redazione, eventualmente a mezzo di CTU, con valutazione giudiziale diretta delle caratteristiche oggettive di qualità e sicurezza; il che fa ritenere che l'eventuale disconoscimento della firma elettronica non comporterà tuttavia l'onere per la parte che voglia utilizzare il documento di instaurare il procedimento di verifica, con

inapplicabilità degli artt. 214 – 215 c.p.c., e degli effetti sanciti dall'art. 2702 c.c.

Ciò presuppone, quindi, che il riconoscimento del requisito di forma scritta “abiliti” l'applicabilità degli artt. 633 e 634 c.p.c. ai fini della ammissibilità della prova nella fase monitoria, laddove il disconoscimento potrà sempre farsi valere nella fase di opposizione e, più in generale, debba inquadarsi negli effetti *ad substantiam* del negozio e cioè conferisca il valore di prova legale ogni qualvolta la legge preveda il requisito di forma scritta indispensabile per la validità dell'atto.

Così descritta pertanto la firma elettronica leggera si inquadrerebbe come un *tertium genus* nell'ambito delle prove documentali codicistiche: se infatti, come vedremo, firma digitale ed elettronica avanzata assurgono a rango di scrittura privata riconosciuta, mentre il documento informatico non sottoscritto è equiparabile alle riproduzioni meccaniche e pertanto costituisce piena prova, salvo disconoscimento e conseguente libera valutabilità giudiziale al pari di queste ultime, non così chiara è la posizione della forma intermedia: il documento sottoscritto con firma elettronica semplice o leggera.

Da quanto abbiamo premesso apparirebbe infatti una diversa configurazione rispetto alla scrittura privata non riconosciuta: quest'ultima infatti una volta disconosciuta può acquistare valore di prova solo a seguito del vittorioso esperimento della procedura di verifica, essendo preclusa al giudice ogni diversa valutazione. Al contrario, per la firma elettronica leggera, il legislatore del 2000 non solo ha escluso l'espressa equiparazione alla scrittura privata, ma nel prevedere la libera valutazione giudiziale “tenuto conto delle sue caratteristiche di qualità e sicurezza”, sembrerebbe avere escluso la possibilità di disconoscimento; fatto inaccettabile per la prevalente dottrina che riterrebbe violati i più elementari principi di difesa garantiti dall'art. 24 co. 2 Cost..

In questa prospettiva possiamo invece concludere ritenendo che il legislatore abbia voluto assegnare al documento informatico munito di firma elettronica semplice un'efficacia probatoria particolare proprio in considerazione dell'incertezza dell'autenticità della relativa sottoscrizione: allorquando il documento sottoscritto con firma elettronica semplice non venga disconosciuto, avrà valore di piena prova, mentre qualora venga disconosciuto o comunque contestato, potrà essere liberamente valutabile in giudizio secondo il grado di certezza che la firma può garantire nel singolo caso.

c - documento informatico, sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata e/o qualificata.

Il documento informatico, sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata e/o qualificata “*quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto*”.

Venuto meno, con il richiamo all'art. 2702 c.c., ogni riferimento all'onore di riconoscimento o disconoscimento della sottoscrizione (e del collegato procedimento di verifica), la pienezza della prova conferita al documento informatico sottoscritto con firma digitale può essere messa in discussione soltanto mediante l'esercizio della querela di falso.

L'efficacia di piena prova del documento sottoscritto con firma digitale deve intendersi riferita unicamente alla provenienza dell'atto, con la logica conseguenza secondo cui il contenuto sarà in ogni caso sottoposto al principio della libera valutazione (art. 116 c.p.c.), sicché ogni mezzo di prova potrà essere utilizzato per dimostrarne il contrario.

Anche perché se si ritenesse la piena efficacia probatoria operante non solo per la provenienza dell'atto, ma anche quanto all'autenticità e integrità del contenuto, si toglierebbe ogni significato all'autenticazione della sottoscrizione del documento informatico da parte del notaio (art. 24 d.P.R. 445/2000).

Del pari, anche gli altri aspetti essenziali – quanto all'efficacia probatoria – e cioè quelli dell'avvenuta ricezione e spedizione, nonché della data e dell'ora di formazione, di trasmissione o di ricezione del documento informatico (di cui all'art. 14 TU) non risultano coperti dalla piena efficacia probatoria di cui al citato art. 10 comma 3 saranno quindi rimessi al principio della libera valutazione (art. 116 c.p.c.).

d - documento informatico con firma digitale autenticata.

L'art. 24 del d.P.R. 445/2000 fa riferimento esplicito alla *firma digitale*, ma può sostenersi l'applicabilità dell'autenticazione notarile anche al documento informatico sottoscritto con altro tipo di *firma elettronica avanzata*.

La funzione probatoria che l'art. 24 del d.P.R. 445/2000 affida al documento in esame si risolve nella prova – controvertibile soltanto con la querela di falso avverso le relative attestazioni notarili – della: a) provenienza della firma digitale dal suo titolare, preventivamente identificato; b) validità della chiave (o della certificazione) utilizzata; c) dichiarata corrispondenza tra la volontà espressa nel documento e quella che s'intendeva manifestare; d) non contrarietà dell'atto all'ordinamento giuridico a norma della legge notarile (assenza di vizi cagionanti la nullità); e) provenienza dell'atto dal pubblico ufficiale; f) data.

L'intervento del notaio assumerebbe, perciò, la finzione di restringimento o comunque modificare l'oggetto del possibile giudizio di falso instaurato contro il documento informatico. Infatti, ove venga prodotto in giudizio un documento informatico con firma digitale autenticata, la parte contro cui è prodotto potrà proporre querela di falso per far valere la mendacità delle dichiarazioni del pubblico ufficiale, non per far valere semplicemente che la sua chiave privata è stata abusivamente o fraudolentemente utilizzata da altri a sua insaputa. Ciò comporta, indubbiamente, un rafforzamento della tenuta probatoria del documento informatico sottoscritto con firma digitale autenticata.

5. Valore ed efficacia probatoria del documento informatico nel d.lgs. 82/2005 (c.d. C. A. D.) e relative modifiche

Con l'entrata in vigore del Codice dell'amministrazione digitale (gennaio 2006), attraverso il d.lgs. 82/2005, il valore probatorio del documento informatico ha subito una ulteriore modifica, difatti con il co. 2 dell'articolo 21, come modificato dal d.lgs. 159/2006, è stabilito che *"Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 c.c.. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria."*

Il citato decreto legislativo rivede anche le tipologie di firma elettronica previste contemplando tre tipologie di firma:

1- firma elettronica;

l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

2 - firma elettronica qualificata;

la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

3 - firma digitale;

un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le norme continuano a contemplare due tipologie di certificato (qualificato e non qualificato) e tre di certificatore (che rilascia certificati qualificati: accreditato o notificato; che rilascia certificati non qualificati). Istanze e dichiarazioni inviate per via telematica da e verso la PA sono valide se sottoscritte mediante firma digitale basata su un certificato qualificato rilasciato da un certificatore accreditato e generata mediante un dispositivo sicuro per la creazione di firme elettroniche.

Nella sua originaria versione, il CAD prevedeva che il solo documento informatico sottoscritto con firma elettronica qualificata o con firma digitale fosse in grado di soddisfare il requisito legale della forma scritta, mentre analoga idoneità era preclusa al documento informatico cui fosse apposta una firma elettronica semplice.

Ne derivava quel paradosso giuridico per cui ci si trovava in presenza di un documento cui, pur essendo stata validamente apposta una firma (o quanto meno pur essendo stata compiuta rispetto ad esso un'attività che lo stesso Legislatore qualificava con il nomen iuris di "firma"), si considerava come non firmato.

Con il decreto correttivo del 17 marzo 2006, il Legislatore ha nuovamente modificato l'assetto normativo, inserendo all'articolo 20 del c.a.d. un co. 1-bis che così recita: *"L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2"*.

Il co. 2 dell'articolo 20, anch'esso parzialmente modificato, stabilisce che *"Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, numeri da 1 a 12 del codice civile"*.

La nuova disciplina relativa all'efficacia probatoria del documento informatico firmato, recuperando il rinvio pieno ed esplicito all'art. 2702 c.c., realizza opportunamente il superamento delle tesi secondo le quali la natura dei documenti informatici firmati sarebbe incompatibile con la disciplina delle scritture firmate tradizionali. Tale disciplina, infatti, non trova fondamento nella natura del supporto materiale utilizzato per la documentazione o in quella dei segni impressi allo stesso, ma nella funzione probatoria che tali materiali e segni sono idonei a soddisfare.

Com'è noto, questa funzione è legata, in primo luogo, alla natura di contrassegno propria della firma apposta sul documento, cioè alla sua essenza di prova critica precostituita nel momento stesso della documentazione, prima ancora che possa sorgere qualsiasi questione in merito alla provenienza del documento. Per mezzo di tale prova, finché esiste il documento, in caso di controversia o anche di semplice dubbio sulla provenienza del documento è possibile dimostrare criticamente che esso è stato formato dal soggetto indicato. Ciò consente di argomentare che il documento è autentico.

In secondo luogo, la funzione probatoria delle scritture private è legata alla scarsa probabilità che soggetti eventualmente interessati ad una falsificazione riescano ad alterare lo stato originariamente conferito al documento per mezzo dall'attività di documentazione, senza che tale intervento lasci una traccia rilevabile per mezzo di un'ispezione diligente. Ciò rende il documento idoneo a dimostrare ragionevolmente - anche se non inconfutabilmente - che il contenuto che appare al momento dell'ispezione è conforme quello che era stato conferito allo stesso nel momento della sua formazione, cioè consente di argomentare che il documento è genuino.

Invece, non è necessario:

a) né che l'illazione dal segno di firma al suo autore sia basata sulla massima di esperienza secondo la quale non esistono due grafie uguali, come accade nel caso delle firme chirografe;

b) né che le alterazioni del contenuto originario del documento si ricavano dalla rilevazione di cancellature, abrasioni o simili, come accade nel caso delle scritture tradizionali.

A tali condizioni, per conoscere la provenienza delle scritture si può svolgere a ritroso la prova critica preconstituita mediante l'apposizione del contrassegno di firma, per risalire, mediante lo strumento della prova per presunzioni, dalla constatazione della presenza e delle caratteristiche del segno di firma alla conoscenza del fatto, altrimenti ignoto, che quel segno è stato apposto per autorità del soggetto indicato, il quale si è reso in tal modo autore del documento firmato.

Nel caso delle firme chirografe, la funzione di contrassegno è resa possibile dalle caratteristiche obiettive del segno personale di sottoscrizione. Nel caso delle firme elettroniche qualificate, ciò è reso possibile dalle caratteristiche tecniche del dispositivo di firma e del procedimento informatico di cifratura (sottoscrizione) e decifrazione (verificazione) del testo firmato. Tali elementi, infatti, garantiscono ragionevolmente il controllo del titolare sull'uso della firma a lui intitolata.

Da tali considerazioni si ricava che, date le sue caratteristiche obiettive, se una firma chirografa risulta compatibile con il campione di comparazione con il quale è stata verificata è molto più probabile che sia autentica, piuttosto che contraffatta. Allo stesso modo, date le caratteristiche obiettive di una firma elettronica qualificata, qualora la verifica informatica dia esito positivo, è molto più probabile che tale firma sia autentica, piuttosto che contraffatta.

L'art. 2702 c.c. dispone che la verifica del contrassegno di firma è necessaria solo se la questione dell'autenticità del documento risulta effettivamente controversa. In caso di riconoscimento della firma, invece, il fatto dell'autenticità si dà per non contestato e, quindi, non deve essere provato: tale è la rilevanza del riconoscimento della sottoscrizione.

A tali condizioni, non appare ragionevole ritenere che il riconoscimento delle firme elettroniche sarebbe irrilevante o superfluo, perché anche nel caso delle firme elettroniche si pone la medesima alternativa che si pone per quelle tradizionali: se l'autenticità del documento è affermata da entrambi i litiganti, essa non deve essere provata. Se invece tale circostanza risulta controversa, non ci si può limitare a considerare il valore indicativo della firma, ma si deve esaminare anche il suo valore probatorio, svolgendo criticamente a ritroso il ragionamento reso possibile dalla sua natura obiettiva di prova critica preconstituita.

Nel caso delle scritture tradizionali, l'autenticità dell'indicazione di provenienza è riconoscibile criticamente tramite la comparazione della firma con un campione di provenienza certa. Nel caso delle firme elettroniche, tale

conoscenza è resa possibile dalla verifica informatica della firma mediante applicazione della chiave pubblica certificata validamente.

A tal fine è necessaria la verifica informatica, ai fini della quale, com'è noto, non è sufficiente applicare la chiave pubblica alla firma da verificare, ma è necessario confrontare i dati riportati nel certificato allegato al documento originariamente ricevuto con quelli aggiornati, che si ricavano consultando l'ultima versione del repertorio di certificati curato dal certificatore.

Tale verifica deve essere compiuta dal giudice su istanza di colui che ha prodotto il documento in giudizio in base alla disciplina contenuta negli artt. 214 ss. c.p.c. (spec. artt. 216 ss.).

Alla luce di tali considerazioni, il rinvio pieno e incondizionato dall'art. 21, co. 2 del c.a.d., l'art. 2702 c.c. va interpretato nel senso che la disciplina delle scritture private tradizionali e di quelle elettroniche munite di firma qualificata è la medesima. Infatti:

- a) in entrambi i casi la mera produzione del documento in giudizio non consente la formazione di alcuna prova in ordine alla provenienza del documento;
- b) tale prova non è necessaria, se l'autenticità del documento risulta non controversa per effetto del riconoscimento compiuto dalla parte contro la quale il documento è prodotto;
- c) in caso contrario, non ci si può limitare a prendere atto dell'indicazione offerta dalla firma, ma è necessario verificare la veridicità di tale indicazione;
- d) la prova di tale circostanza è a carico di colui che ha interesse a far valere il documento, cioè di colui che lo ha prodotto in giudizio, perché egli dispone di una prova critica appositamente preconstituita a tale scopo sin dal momento della creazione del documento, cioè il contrassegno di firma;
- e) il giudizio di verifica è regolato dagli artt. 214 ss. c.p.c. (spec. artt. 216 ss.).

In definitiva, qualsiasi firma consiste in una indicazione di provenienza che ha valore dichiarativo ed è suscettibile di verifica. Anche la firma elettronica, come quella tradizionale, ha le caratteristiche obiettive di un contrassegno e, per tale ragione, non solo esprime una dichiarazione di provenienza, ma consente di verificare criticamente quella provenienza.

In entrambe le ipotesi, in caso di disconoscimento, colui che ha interesse a far valere la scrittura deve chiedere la verifica della loro autenticità. A tal fine può fornire qualsiasi prova idonea (art. 216 c.p.c.), ma se ha conservato la disponibilità del documento, egli ha a sua disposizione la prova per presunzioni basata sul contrassegno di firma, e cioè, nel caso delle firme tradizionali, ha quella basata sulla comparazione delle scritture, e, nel caso delle firme elettroniche qualificate, ha quella basata sulla verifica informatica. Raggiunta tale prova, colui contro il quale la scrittura è prodotta, se ne ha a disposizione, può sempre fornire qualsiasi prova contraria.

La precisazione contenuta nell'art. 21, co. 2 c.a.d. non sposta tale conclusione, ma contribuisce in maniera decisiva a rassicurare chi teme che la

verificazione informatica, pur essendo idonea a dimostrare ragionevolmente che la firma controversa è stata generata usando il dispositivo di firma attribuito al titolare, non sarebbe sufficiente a far presumere anche la riconducibilità di tale utilizzo alla volontà del medesimo.

Per scongiurare definitivamente tale timore, il legislatore ha avuto cura di precisare che «l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria».

CAPITOLO II

FABIEN DESIO PRESUTTI

UTILIZZO DEL SOFTWARE OPEN SOURCE NELLA P.A.

SOMMARIO: 1. Introduzione. – 2. Open source e Free software, definizioni e differenze. – 3. Open Source e diritto d'autore. – 4. Le licenze di software libero, la GPL. – 5. Open source e P.A. - Quadro storico di riferimento. – 6. La direttiva sull'Open Source. – 7. L'Osservatorio Open source presso il CNIPA. – 8. La situazione nelle P.A.L. – 9. I vantaggi per la P.A. – 10. La questione economica - Il Value Management. – 11. La situazione e le iniziative in Europa. – 12. La direttiva sull'Open Source in Francia. 13 – La direttiva sull'Open Source in Germania. – 14. Formati aperti e formati standard. – 15. Il formato Open Document Format (ODF). - 16. Il caso Open Office.org – 17. L'espansione di ODF e Open Office.org. – 18. Considerazioni conclusive.

1. Introduzione

Scopo del presente lavoro è quello di analizzare il fenomeno dell'Open source (OS), il software cioè a codice sorgente aperto, ed in particolare, quanto il suo utilizzo possa apportare vantaggi per la PA da un punto di vista non solo prettamente economico.

Lo studio parte con l' esaminare il funzionamento dell'OS e le sue differenze con il Free software. Si prosegue approfondendo i suoi rapporti con la PA, e la normativa che per prima ne ha evidenziato gli aspetti innovativi, la Direttiva del 19 dicembre 2003 (G.U. 7 febbraio 2004 n. 31), la quale indica come bisogna favorire l'utilizzo di prodotti informatici che promuovano il pluralismo del software e quindi la possibilità di scegliere tra le soluzioni più convenienti, non solo in termini economici, tra quelle esistenti sul mercato, soluzioni inoltre che permettano il riuso delle applicazioni da parte di altre Amministrazioni diverse da quelle committenti.

Viene presa in considerazione la questione legata all'acquisto di software da parte della PA, introducendo al concetto di Value Management e di Total Cost of Ownership (TCO - Costo totale del possesso).

In seguito viene presentata la situazione e le iniziative in Europa, più in particolare di Francia e Germania, gli Stati che più degli altri hanno mostrato interesse nei confronti del mondo del software OS e del suo coinvolgimento nelle tematiche del settore pubblico. La ricerca prosegue con l'analisi dei formati file "aperti", in particolare del formato Open Document Format (ODF) che garantisce l'accesso ai dati a lungo termine senza barriere legali o tecniche essendo un'alternativa "aperta" ai formati di file proprietari, una caratteristica che svincola le Amministrazioni pubbliche e le aziende private dal rimanere legate a tecnologie di esclusivo possesso di un soggetto privato e dà loro garanzia che tutti i propri documenti potranno sempre essere aperti e modificati. Non è infatti auspicabile lasciare nelle mani di una singola azienda

gli standard pubblici di Information Technology (IT). Si conclude con l'analizzare il caso e l'espansione continua di OpenOffice.org, la prima suite per ufficio OS in grado di competere con Ms Office, che adottando il formato aperto ODF sta sempre più prendendo piede nelle Pubbliche Amministrazioni europee ed extraeuropee.

2. Open source e Free software, definizioni e differenze.

L'origine di quel complesso fenomeno che va sotto il nome di Open Source è intimamente connessa con la storia del sistema operativo UNIX. La comunità scientifica creatasi con la prima fase di sviluppo di UNIX, quando tramontò l'idea di un suo sviluppo non proprietario aveva maturato al suo interno una forte coesione intellettuale e un modello culturale di collaborazione. Si ricostituì, infatti, parzialmente nella Free Software Foundation (FSF) creata da Richard Stallman e poi nella Open Source Initiative (OSI).¹

I due movimenti che ne sono derivati, quello del software libero (free software) e quello del codice a sorgente aperto (open source), condividono entrambi l'idea guida della disponibilità completa senza limitazione dei sorgenti, ma si diversificano, oltre che per la terminologia, per alcuni aspetti filosofici e di principio. In particolare, la definizione di software proposta dalla FSF recita testualmente: "L'espressione software libero si riferisce alla libertà dell'utente di eseguire, copiare, distribuire, studiare, cambiare e migliorare il software. Più precisamente, esso si riferisce a quattro tipi di libertà per gli utenti:

- Libertà di eseguire il programma, per qualsiasi scopo (libertà 0)
- Libertà di studiare come funziona il programma e adattarlo alle proprie necessità (libertà 1). L'accesso al codice sorgente ne è un prerequisito
- Libertà di ridistribuire copie in modo da aiutare il prossimo (libertà 2)
- Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti, in modo tale che tutta la comunità ne tragga beneficio (libertà 3). L'accesso al codice sorgente ne è un prerequisito.

Secondo la FSF il software deve essere libero non in quanto gratuito ma per una questione etica e di principio. Esistono una serie di diritti dell'utente del software che devono essere adeguatamente tutelati: il software deve essere "libero" per questi motivi prima ancora che per motivi di carattere economico e di mercato.² La comunità del software Open Source condivide in larga misura le posizioni del mondo del software libero, ma deenfatisa gli aspetti etici, fondando le proprie scelte e motivazioni su considerazioni di carattere tecnico-economico. Secondo i sostenitori del software Open Source, tali

¹ "Open source e PA", di Giovanni Sissa, Mondo Digitale n. 3, 2003

² "Indagine conoscitiva sul software a codice sorgente aperto nella PA", <http://www.innovazione.gov.it>.

motivazioni tecnico-economiche sono sufficienti a giustificare la necessità del software aperto/libero.³

In particolare, il Free software antecedente all'Open Source sottolineava il carattere etico e solidaristico, mentre l'Open Source, più recente, pur aderendo agli ideali filosofici libertari del Free software sottolinea in misura maggiore gli aspetti pratici e pragmatici del suo utilizzo.⁴ Il primo aspetto assolutamente pragmatico è la disponibilità del codice sorgente, ossia della sintassi con cui esso è stato elaborato, in modo da rendere palese il suo funzionamento ed, eventualmente, consentirne il miglioramento adattandolo ad esigenze diverse da quelle per cui era stato pensato.

Il Software Open Source non è un'alternativa al software commerciale. Open Source non vuol dire gratis, ma indica un modello che si pone in alternativa al modello proprietario (closed source) il quale concede all'utente solo una licenza di utilizzo senza alcuna possibilità di modificare il codice sorgente. Un programma è invece Open Source se l'utente, o chi per lui, ha la possibilità di studiare il codice, di modificarlo o di riassemblarlo adattandolo alle proprie necessità e, soprattutto di ridistribuirne sia la copia originale che quella modificata, utilizzando le modalità che si ritengono più opportune.⁵

I criteri dell'Open Source Iniziative (OSI) che permettono di determinare la natura libera o proprietaria di una licenza di software si articolano in nove punti:

1. libertà di redistribuzione
2. codice sorgente
3. prodotti derivati
4. integrità del codice sorgente dell'autore
5. assenza di discriminazione nei confronti di persone o gruppi
6. assenza di discriminazione nei confronti di sfere di attività
7. distribuzione di licenza
8. la licenza non deve essere specifica di un prodotto
9. la licenza non deve imporre limitazioni ad altri software: ovvero, esigere che gli altri programmi distribuiti sullo stesso supporto fisico siano anch'essi software libero.

Una licenza software è "ufficialmente" Open Source a discrezione dell'OSI: se una licenza segue le linee guida dell'OSI, allora tale licenza può essere dichiarata licenza open source, ma le direttive potrebbero cambiare nel tempo, è quindi possibile che una licenza attualmente OS non lo sia nel futuro o viceversa. Una licenza è invece libera se e solo rispetta le quattro libertà fondamentali.⁶ Pertanto se una versione di una licenza è libera lo sarà per sempre.

³ Art. cit.

⁴ "Questione di libertà o sviluppo? – Ne parliamo con Arturo di Corinto, docente di Comunicazione mediata dal computer presso l'Università degli Studi la Sapienza di Roma", <http://www.forumpa.it>.

⁵ "Open Source: continua il dibattito", <http://www.forumpa.it>.

⁶ <http://it.wikipedia.org>.

3. Open source e Diritto d'autore

Il software Open Source, in quanto opera dell'ingegno, rientra nella legge sul Diritto d'Autore, ed è regolato e disciplinato dalla legge n. 633 del 1941 e successive modificazioni introdotte dal D.lgs. n. 68 del 2003 (Attuazione della Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione).

A seguito della diffusione del software OS, si è reso necessario definire nuove direttive per regolare la diffusione di questo tipo di prodotto. La fonte primaria per la regolamentazione del Diritto d'Autore è la succitata Legge 633/41, su cui è intervenuta specificamente, per quanto riguarda il software, il provvedimento comunitario 91/250/CE sulla tutela giuridica del software, modificata dalla Direttiva 93/98/CE del Consiglio; e ai sensi della legge sul Diritto d'Autore e il D. lgs. 518/92 di recepimento (modificata dalla Legge n. 248/00 "Nuove norme di tutela del Diritto d'Autore").

Il software OS è dunque compatibile con la legislazione italiana, che già prevede la protezione del diritto d'autore, vale a dire la tutela del segreto e della proprietà intellettuale frutto del lavoro di aziende o di singoli professionisti.⁷La differenza tra il software OS e quello proprietario non riguarda quindi la protezione del diritto d'autore, ma solo ed esclusivamente le modalità di rilascio dello stesso all'utente. Nel primo caso si rilascia sempre all'utente anche il codice sorgente ed alcuni diritti che l'autore concede anche a terzi, non riservandosi in maniera esclusiva, mentre nel secondo caso si rilascia soltanto il programma eseguibile (codice oggetto – file.exe).⁸Quindi il software OS consente all'utente un maggior controllo sui lavori svolti dal fornitore di software, mentre con il software proprietario questo controllo non è possibile, a meno di accordi specifici con il fornitore che autorizzino l'utente ad accedere al codice sorgente.

4. Le licenze di software libero, la GPL

Le licenze di software libero consistono in una messa a disposizione del software con l'intento di permettere la libera evoluzione del software medesimo. La licenza non ha per scopo il trasferimento di un diritto di proprietà o la rinuncia al diritto d'autore o di far cadere il software nel "pubblico dominio".

Diffondendo il proprio software libero l'autore può assicurarsi che la libera utilizzazione del software non sia perturbata dall'azione dei soggetti alla licenza.⁹Richard Stallman e la FSF definiscono il concetto di **copyleft** in contrapposizione al tradizionale copyright: ove quest'ultimo tende a tutelare il diritto d'autore, anche attraverso limitazioni alla conoscenza, il copyleft

⁷ "Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -", <http://www.cnipa.gov.it>.

⁸ Op. cit.

⁹ "Open Source e PA", di Giovanni Sissa, Mondo Digitale n. 3, settembre 2003

intende tutelare il più generale diritto della collettività a fruire dei prodotti dell'innovazione.

I principi del copyleft vengono formalizzati dalla FSF nella cosiddetta **General Public License (GPL)**. Il cliente di accordo GPL è vincolato ad utilizzare a sua volta la GPL e dovrà, quindi, fornire il codice sorgente delle estensioni realizzate. In altre parole la GPL è un modello di licenza ricorsivo, il codice e le libertà ad esso associate diventano così legalmente inseparabili. Il mondo dell'OS non coincide con la GPL. Esistono modelli di licenza alternativi, quali ad esempio: LGPL (lesser general public license); BSD (Berkley Software Distribution); MPL (Mozilla Public License) che prevedono in modo diverso l'apertura del codice. Alcune licenze, come la GPL vietano la realizzazione di soluzioni proprietarie a partire da software libero, altre invece, come la BSD, consentono derivazioni proprietarie.

5. Open source e P.A. - Quadro storico di riferimento

Già agli inizi del 2000, rappresentanti dell'allora AIPA (ora CNIPA), del Ministero della Pubblica Istruzione, dell'ALCEI e della rivista Interlex sostenevano che lo Stato era troppo dipendente dai prodotti Microsoft contraddistinti da costi piuttosto elevati. Si sosteneva che i prodotti "incriminati" erano soggetti a rapidi aggiornamenti tra l'altro incompatibili con versioni precedenti, ciò imponeva come logica conseguenza, degli onerosi finanziamenti per l'approvvigionamento di nuovo software.¹⁰

Questo movimento con il passare del tempo si è ulteriormente organizzato fino alla nascita di una vera e propria associazione per la diffusione del software Open source nella PA denominata "Associazione OpenPA". Le numerose attività favorevoli all'introduzione del software Open source nella PA produssero gli effetti voluti ed il Ministro per l'Innovazione e le Tecnologie resosi conto di questa importante realtà costituì con Decreto firmato il 31 ottobre 2002 una Commissione di esperti (Commissione per il software a sorgente aperto nella PA), con l'obiettivo preciso di procedere ad un'analisi dettagliata delle opportunità per le PA derivanti dall'Open source.

Il lavoro della Commissione ha portato alla pubblicazione dell'"Indagine conoscitiva sul software Open source nella PA" contenente alcune proposte concrete per favorire la diffusione del software Open source nella PA italiana.¹¹ Questo studio porterà all'emanazione della Direttiva del 19 dicembre 2003 (Sviluppo ed utilizzazione dei programmi informatici da parte della PA).

6. La Direttiva sull'Open source

La possibilità di acquisizione ed utilizzo di programmi informatici Open Source da parte della Pubblica Amministrazione viene sancita con la

¹⁰ "Open source nella PA, ci sarà un futuro?", Michele Iaselli, <http://www.studiocelentano.it>.

¹¹ <http://www.ossipa.cnipa.it>

pubblicazione della Direttiva del 19 dicembre 2003 “Sviluppo ed utilizzazione dei programmi informatici da parte della PA” (G.U. 7 febbraio 2004 n. 31) predisposta dal Ministro per l’Innovazione e le Tecnologie. Essa intende fornire alla PA indicazioni e criteri tecnico operativi per gestire più efficacemente il processo di predisposizione o di acquisizione di programmi informatici.¹²L’atto è stato preceduto da una approfondita indagine conoscitiva condotta da una apposita Commissione tecnica che, per la prima volta, ha fotografato la situazione dell’informatica e del software OS nella PA. In particolare, viene indicato come le PA debbano tener conto dell’offerta sul mercato di una nuova modalità di sviluppo e diffusione dei programmi informatici a codice sorgente aperto.

L’inclusione di questa nuova tipologia di offerta all’interno delle soluzioni tecniche tra cui scegliere, contribuisce ad ampliare la gamma delle opportunità e delle possibilità in un quadro di economicità, equilibrio, pluralismo e aperta competizione.¹³Si tratta di favorire l’utilizzo di prodotti informatici che promuovano il pluralismo del software nella PA e quindi, la possibilità di scegliere tra le soluzioni più convenienti non solo in termini economici tra quelle disponibili sul mercato. Con riferimento agli art. 3 a art. 4 e art. 7, il primo aspetto da considerare è che la Direttiva non intende stravolgere le usuali procedure di acquisizione dei programmi informatici da parte delle amministrazioni pubbliche, come rappresentato dal riferimento alle leggi 241/90 e 39/1993. Esaminando l’articolo 3, la novità più significativa è rappresentata dall’elenco di soluzioni tecniche possibili che includono, per la prima volta esplicitamente, il riuso di applicazioni sviluppate per altre amministrazioni ed i programmi Open source.

Secondo quanto espresso dalla Direttiva, le amministrazioni che intendano dotarsi di un sistema informatico dovranno effettuare e riportare nello Studio di Fattibilità una comparazione tra le soluzioni disponibili sulla base anche dei seguenti elementi:

- TCO (Costo Totale del Possesso) della singola soluzione
- Costo uscita dalla stessa (lock in)
- Valorizzazione delle competenze tecniche possedute dall’amministrazione
- Interoperabilità intesa nella PA nel suo complesso (uso di formati e interfacce aperte e standard)
- Interesse di altre amministrazioni al riuso dell’applicazione e/o acquisto.

La Direttiva non entra nel merito di come eseguire la comparazione di cui sopra: afferma soltanto che la stessa sarà oggetto di valutazione da parte del CNIPA in sede di rilascio del Parere di Congruità tecnico/economica.¹⁴ L’art. 4, fornisce una serie di caratteristiche sulla base delle quali motivare la

¹² <http://www.ossipa.cnipa.it>

¹³ “Stanca emana la Direttiva per l’open source nella PA”, Comunicato stampa del 29/10/2003 a cura dell’Ufficio Stampa del Ministero per l’Innovazione e le tecnologie.

¹⁴ “Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto - ”, <http://www.cnipa.gov.it>.

scelta di soluzioni informatiche da parte delle amministrazioni. Nessuna di tali caratteristiche è qualificata dalla Direttiva come obbligatoria, tuttavia la loro presenza viene indicata come criterio di preferenza. In sintesi, le caratteristiche tecniche indicate sono:

- uso di standard aperti per dati e interfacce
- indipendenza da tecnologie proprietarie o dipendenti da un unico fornitore
- disponibilità del codice sorgente per ispezione e tracciabilità
- capacità di esportare dati e documenti in formato aperto.

Nel caso di acquisizione di programmi informatici di tipo proprietario mediante il ricorso a licenze d'uso, le amministrazioni si debbono contrattualmente assicurare che, qualora il fornitore non sia più in grado di fornire supporto, il codice sorgente e la relativa documentazione vengano resi disponibili o almeno ceduti dal fornitore.

Nel caso di programmi sviluppati ad hoc (custom), l'amministrazione committente ne acquisisce la proprietà dato che ha contribuito con le proprie risorse all'identificazione dei requisiti, all'analisi funzionale, al controllo ed al collaudo del software realizzato dall'impresa fornitrice. Le PA, inoltre, si assicurano contrattualmente la possibilità di trasferire la titolarità delle licenze dei programmi informatici acquisiti nelle ipotesi in cui all'amministrazione che ha acquistato la licenza ne subentri un'altra nell'esercizio della stessa attività.

Per favorire il riuso del software di proprietà delle amministrazioni, nei capitolati e nelle specifiche di progetto dovrà essere previsto che i programmi sviluppati ad hoc siano facilmente esportabili su altre piattaforme.¹⁵ Inoltre nei contratti di acquisizione dei software sviluppati per conto e a spese delle amministrazioni, le stesse includono clausole che vincolano il fornitore a mettere a disposizione servizi che consentono il riuso delle applicazioni.

7. L'Osservatorio Open source presso il CNIPA

Considerando il particolare rilievo che l'utilizzo del software Open source (ossia qualsiasi sistema di gestione delle informazioni e delle comunicazioni che consente la disponibilità del codice sorgente) sta assumendo tra i fenomeni significativi legati allo sviluppo dell'ICT, Il CNIPA in attuazione della Direttiva del Ministro per l'Innovazione e le Tecnologie del 19 dicembre 2003 (G.U. 7 febbraio 2004 n. 31) ha costituito l'**Osservatorio Open Source**.¹⁶

L'Osservatorio è un punto privilegiato di osservazione su un fenomeno ancor poco chiaro che spesso viene considerato troppo legato ad ideali e ad utopie, e poco allo sviluppo economico ed industriale.¹⁷ Gli obiettivi dell'Osservatorio sono:

¹⁵ "Open source nella PA, ci sarà un futuro?", Michele Iaselli, <http://www.studiocelentano.it>.

¹⁶ <http://osspa.cnipa.it>.

¹⁷ "Open source: il dibattito continua", <http://forumpa.it>.

- Lo studio e la diffusione delle politiche di licensing sui prodotti Open source, compatibili con le esigenze della PA
- La promozione di iniziative volte a diffondere il patrimonio di esperienze – in ambito Open source – già maturate o in fase di sviluppo presso le università ed i Centri di ricerca nazionali
- La creazione di strumenti on line atti a favorire l’incontro tra domanda ed offerta di prodotti/servizi OS per le PA
- La predisposizione di attività di supporto alle PA relativamente sia ad eventuali adozioni di software OS, sia ad indagini conoscitive attinenti all’Open source su specifiche tematiche
- La promozione e lo scambio di esperienze con gli analoghi Centri operanti nei paesi UE.

All’interno dell’Osservatorio ruota il **Centro di Competenza** “Open Source”. Questo svolge un importante funzione di catalizzatore delle “best practice” e della conoscenza in materia di OS.

Le infrastrutture e l’organizzazione del Centro favoriscono l’accentramento di conoscenze ed esperienze e la diffusione del know-how nella PA, grazie anche alla promozione di processi di valutazione e comparazione di software. Gli obiettivi perseguiti dall’Osservatorio, e le linee di azione attuate dal Centro non solo sono allineati a quelli dei principali Paesi europei (esistono nell’UE Centri di Competenza assimilabili a quello italiano) ma rientrano tra le iniziative che furono auspicate dal programma UE IDA (Interchange of Data between Administrations). Le principali attività del Centro di Competenza sono:¹⁸

- Mettere a disposizione forum di discussione in materia di OS aperti agli utenti, pubblicare i risultati delle rilevazioni sull’uso dell’OS, nonché studi specifici in materia
- Studiare tipologie di licenze d’uso e di contrattualistica per prodotti e servizi OS, adeguate per l’impiego nelle PA (es. capitolati di gara)
- Fornire supporto alle PA dove richiesto
- Svolgere azioni di verifica, di mantenimento e di miglioramento del software OS prodotto ex novo per la PA o frutto di riuso
- Gestire una vetrina di prodotti OS per la PA, accessibile presso il portale del CNIPA, al fine di diffondere la conoscenza del software OS e di facilitare l’incontro tra la domanda di soluzioni tecnologiche e l’offerta di prodotti e servizi in ambito OS.

Il Centro di Competenza si pone come struttura essenziale per il conseguimento degli obiettivi configurandosi come punto di riferimento e collettore dei contributi della comunità.

All’interno dell’Osservatorio opera un sistema di **Rilevazione Continua** sull’uso del software OS presso la PA, con il quale si intende creare un canale di comunicazione con le PA, relativamente all’adozione ed all’uso di software Open source da parte delle PA stesse per risolvere le proprie

¹⁸ “L’Osservatorio Open source presso il CNIPA”, <http://www.ossipa.cnipa.it>.

specifiche esigenze. Nella Rilevazione, infatti, si richiedono quali esigenze sono state risolte dalla PA con l'aiuto di soluzioni basate (in tutto o in parte) su software OS. Le esigenze ottenute sono esposte sulla “**Vetrina**” dell'Osservatorio Open source, si intende così creare un “punto di raccolta” tra PA, esigenze, soluzioni e mercato. La Vetrina è il principale strumento di disseminazione dei risultati raggiunti dal Centro di Competenza e in prospettiva uno strumento di riferimento, per le PAC e PAL, per orientarsi in modo semplice e diretto verso i prodotti ed i servizi che il mercato Open source propone.¹⁹

8. La situazione nelle P.A.L.

Le Pubbliche Amministrazioni Locali (PAL) hanno già da tempo colto le opportunità fornite dal software OS e libero non solo sul piano della tecnologia, ma anche e soprattutto su quelli della tutela della sicurezza e della privacy dei cittadini, della libertà della diffusione della conoscenza e dell'informazione, dell'indipendenza dai fornitori e della salvaguardia della pluralità del mercato.

Tutto ciò si è tradotto nelle PAL in iniziative concrete che vanno dall'adozione di atti d'indirizzo, alla migrazione su piattaforme Open, all'organizzazione di momenti di discussione e di approfondimento sul tema.²⁰ In particolare la provincia di Pisa ha organizzato e realizzato il Primo Convegno Nazionale sull'Open source nella PA (marzo 2003) cui hanno aderito 600 persone; ha introdotto sistemi OS per l'erogazione dei propri servizi; ha avviato progetti per il ricondizionamento dell'hardware obsoleto con software libero da destinare a finalità sociali e di cooperazione; sta favorendo l'introduzione di software libero nelle scuole. In generale, le realtà più concentrate che quasi formano dei distretti, sono la regione Lombardia, il Veneto, la Toscana e la regione Emilia Romagna.

La spiegazione di tale diffusione ed interesse che circondano l'OS, è secondo il CNIPA, nel modo in cui gli attori chiave agiscono per l'interesse ed il bene comune e per il progresso tecnologico. Infatti, si può notare la spontanea aggregazione in “poli” di competenza del movimento, sia da parte delle imprese che da parte delle associazioni. Si creano così dei veri network che prendono esempio dalle community, creando sinergie finalizzate alla cooperazione ed ad un miglior allocamento delle risorse e prodotti, in modo da permettere a piccole realtà imprenditoriali di svilupparsi e raggiungere l'affidabilità necessaria per puntare agli enti locali, se non addirittura centrali.²¹

Il Consorzio C.I.R.S. (consortium italicum ratione soluta), ad esempio, è un'organizzazione che punta alla creazione di un centro di competenza del

¹⁹ “Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -”, <http://www.cnipa.gov.it>.

²⁰ “Software open e libero: gli enti locali guidano l'innovazione - dalla provincia di Pisa, assessore Buongiovanni”, <http://www.interlex.it>.

²¹ <http://www.tecnoteca.it>.

software libero e con l'obiettivo di promuovere l'uso di soluzioni RMD (Reuse, Modify, Distribuite) nelle imprese e nelle PA²². Tra i progetti di ampio respiro citiamo "Progetto consiglio", proposto dal Consiglio comunale di Venezia, che oltre ad essere un sito di consulenza per l'introduzione delle nuove tecnologie informatiche nella PA, ha realizzato un software "progettoconsiglio" che è stato realizzato con l'obiettivo di offrire l'opportunità a tutti i Consiglieri comunali di dialogare con i cittadini e di rendere pubblico il loro pensiero e il loro operato, software che dal 10 gennaio 2003 è in distribuzione gratuita per i Comuni che ne fanno richiesta.²³ Hanno già richiesto la cessione gratuita del software "progettoconsiglio" i Comuni di Trento, San Donà di Piave (Ve), Giulianova (Te), Rovigo, Osimo (An), Bacoli (Na) e Galatina (Le). Fornire un panorama esaustivo delle esperienze in atto non è agevole per la velocità dei cambiamenti in atto, diremo quindi che l'adozione di tecnologie OS nel territorio italiano è in continua crescita ed è molto probabile che continui in questa direzione.

9. I vantaggi per la P.A.

Il software Open source ha richiamato negli ultimi anni sempre maggiore interesse da parte delle PA. Si sono rivelate decisive in merito allo sviluppo di questa attenzione tre istanze principali:

1. la nascita di applicativi OS di qualità in numerose aree di interesse delle PA
2. alcune caratteristiche cruciali intrinseche al modello di sviluppo stesso di questo tipo di software
3. le potenzialità insite in esso di stimolare l'innovazione nel campo dell'ICT.

Già diversi anni fa il panorama del software libero poteva vantare ottimi programmi nel campo d'infrastruttura. Nell'ambito del networking segnaliamo il web server Apache, il browser Firefox Mozilla, l'application server Zope ed il servizio di posta Sendmail. Tra i sistemi di gestione di database spiccano invece Mysql e PostgreSQL.

Bisognerà aspettare la seconda metà degli anni '90 affinché il software OS possa costituire una alternativa appetibile per le PA nel campo degli applicativi per l'utente finale. Fu solo da quel momento che vennero sviluppate le prime interfacce grafiche per Linux, Gnome e Kde, che hanno permesso l'utilizzo di questo sistema operativo anche agli utenti inesperti.²⁴

Come è noto la PA italiana sta attraversando un periodo particolare contraddistinto dalla rapida diffusione delle nuove tecnologie nei processi organizzativi della PA stessa. Recentemente è entrato in vigore il CAD (Codice dell'Amministrazione Digitale) il cui obiettivo finale è quello di una PA digitale, con protocollo informatizzato, posta certificata e soprattutto

²² <http://www.consorziocirs.it>.

²³ <http://www.progettoconsiglio.it>.

²⁴ <http://www.tecnoteca.it>.

trasparenza dell'iter burocratico verso l'esterno. E' questa l'idea di fondo dell'e-Gov, ma per realizzare un simile processo c'è bisogno di una serie di condizioni che rendano possibile l'integrazione fra le diverse attività e funzioni delle diverse PA e la loro fruibilità da parte dei cittadini. Appare evidente, quindi, che per realizzare gli obiettivi del "governo elettronico" è necessario che si completi quel processo già in atto presso la PA che tende ad ottenere una maggiore efficacia, efficienza, trasparenza e semplicità dell'azione amministrativa grazie all'interazione di un insieme di requisiti infrastrutturali che non sono riconducibili ad una singola amministrazione ma al sistema di relazioni che intercorrono fra le stesse e sono al servizio del cittadino.²⁵

In tale ottica la c. d. **interoperabilità** intesa come l'esistenza di standard di interfaccia tra le amministrazioni che consentano comunicazioni efficienti e trasparenza verso l'esterno, assume una rilevanza fondamentale. Ed in termini di interoperabilità il software OS è sicuramente più adatto del software proprietario. Lo scambio di dati e funzioni tra prodotti diversi implica difatti, in generale, la realizzazione di interfacce, ed in caso di software proprietario solo chi detiene il codice sorgente può realizzare tali interfacce.

L'adozione di software OS può rivelarsi strategica anche in merito alle esigenze di **indipendenza** delle PA. L'apertura dei sorgenti dà alle amministrazioni la possibilità di affidarsi, per il supporto, alle aziende che preferisce evitando di rimanere legata a tempo indeterminato all'azienda produttrice (laddove nel mondo del software proprietario solo il produttore può supportare il proprio software). Può inoltre fornire **maggiori garanzie di sicurezza** rendendo possibile effettuare controlli sulla presenza di banchi o back doors. Allo stesso tempo il software OS è generalmente dotato di una maggiore flessibilità in quanto permette di apportare in maniera semplice delle personalizzazioni, estensioni delle funzionalità e adattamento ad altri sistemi.²⁶

Attraverso l'adozione di software OS le PA potranno beneficiare di una maggiore trasparenza, della possibilità di rimettere in circolo il software creato su misura (custom), della possibilità di stimolare un circolo virtuoso di collaborazione tra Amministrazioni e istituzioni scolastiche e formative, ponendo il software utilizzato al centro dell'analisi e dello studio universitario e scientifico.

In generale i prodotti OS determinano vantaggi per la PA in termini di:

- contenimento dei prezzi
- trasparenza (e quindi sicurezza)
- non dipendenza da un singolo fornitore
- elevata riusabilità
- accessibilità per le piccole realtà di sviluppo (economie locali).

La PA può essere favorita dal modello OS in vari modi, tra i quali, lo sviluppo di infrastrutture software per la connettività multicanale, lo sviluppo

²⁵ "Open source nella PA, ci sarà un futuro?", di Michele Iaselli, <http://www.studiocelentano.it>.

²⁶ <http://www.tecnoteca.it>.

di piattaforme di interoperabilità, di soluzioni specifiche per la PA e di piattaforme strategiche per il Paese (es. e-learning ed e-health).²⁷

Il centro della questione non è, come potrebbe sembrare, né la gratuità né l'economicità, quanto la stabilità, la trasparenza e la sicurezza che questo tipo di software può dare. Il fatto che un software venga distribuito con il suo codice sorgente, infatti, permette a tutti ad esempio, di poter verificare che non vi siano al suo interno funzionalità nocive o dannose, garantendo un corretto rapporto tra PA e cittadini.²⁸

Tra le Amministrazioni e gli Enti ove esistono esempi significativi di impiego di software OS si citano i seguenti casi:²⁹

- La Presidenza del Consiglio dei Ministri, ove è stato sviluppato con tecnologie OS il Portale dei Servizi e, sempre con tecnologie OS, è stato realizzato un sistema di misura del traffico dati
- Il Dipartimento Politiche Fiscali, ove è proseguita la realizzazione di strumenti di collaborazione in ambiente OS
- L'Agenzia del Territorio, ove è stata adottata una soluzione che prevede l'utilizzo per le applicazioni del sistema informativo catastale, di un'architettura web based costituita da Linux, Apache e linguaggio PHP
- L'Agenzia del Demanio, ove viene utilizzato sw OS per la realizzazione del servizio a supporto della gestione dei beni confiscati
- L'INPS sta utilizzando un motore di ricerca a reti neurali, sviluppato con tecnologia OS in alcuni progetti di Knowledge Management, tra cui ad esempio, il progetto NEUWEB, implementazione di un portale per l'accesso a informazioni di sicurezza sociale.

10. La questione economica - Il Value Management.

Uno dei principali argomenti che viene portato a sostegno dell'utilizzo diffuso di software OS è l'ottimizzazione della spesa in tecnologie del software. I sostenitori dell'approccio OS indicano nell'adozione e nella promozione del software OS uno strumento decisivo per ridurre i costi, eliminare duplicazioni di sforzi e velocizzare la diffusione di innovazioni nelle PA. La riduzione della spesa si materializzerebbe nei minori costi di acquisizione iniziale del software, nella possibilità di replicare senza limiti le installazioni.

E' opportuno tuttavia, fare alcune osservazioni sulle caratteristiche dei prodotti software acquisiti dalle PA italiane, al fine di poter meglio valutare il

²⁷ “Linee Guida del Governo per lo sviluppo della Società dell'Informazione”, Roma, giugno 2002.

²⁸ “Questione di libertà o sviluppo? – Ne parliamo con Arturo Di Corinto, docente di Comunicazione mediata dal computer presso l'Università degli Studi La Sapienza di Roma”, <http://forumpa.it>.

²⁹ “Rapporto conclusivo del Gruppo di lavoro -Codice sorgente aperto-”, <http://www.cnipa.gov.it>.

reale impatto che l'approccio OS potrebbe avere.³⁰ Per quanto riguarda il software custom³¹, il problema relativo all'ottimizzazione della spesa deve essere affrontato considerando che nei capitolati di gara deve essere esplicitamente previsto che la proprietà del codice sorgente sia dell'Amministrazione appaltante (almeno in forma non esclusiva). Tale obiettivo può essere raggiunto, quindi, senza alcun particolare riferimento a licenze OS, la piena proprietà del codice offrirebbe garanzie che rendono irrilevante la richiesta che il software sia OS.

La spesa in pacchetti³² software è per sua natura quella più direttamente correlata con il potenziale utilizzo del software OS. I prodotti OS sono spesso disponibili a costi bassissimi e possono essere replicati e installati liberamente dall'utente. Per questo motivo, i sostenitori dell'approccio OS ritengono che l'uso di tali prodotti può portare ad una rilevante riduzione di spesa.

Nelle ultime linee strategiche rilasciate (triennio 2002-2004) esisteva l'obiettivo di migliorare governo e controllo del rapporto con i fornitori al fine di assicurare indipendenza progettuale. Si propose di rafforzare tale obiettivo, introducendo nella modalità di pianificazione della PA il concetto di "Giustificazione economica dell'investimento" (**Value for Money**). Nella realizzazione di un sistema, la giustificazione economica dell'investimento è definita come "la miglior combinazione del **Total cost of Ownership** (Costo complessivo del possesso) del sistema e la sua qualità, intesa come soddisfacimento degli requisiti.

Questo concetto è stato sviluppato proprio per caratterizzare l'insieme dei costi che nel corso dell'intera vita operativa di un pacchetto è necessario sostenere affinché esso sia utilizzabile proficuamente dall'utenza. Non coincide necessariamente con il più basso prezzo di acquisizione. Si propone di raccomandare alle Amministrazioni, nell'acquisizione di soluzioni e servizi di tipo informatico, di prendere decisioni sulla base del **value for money** come fattore principale. Si deve raccomandare l'uso di questo strumento sin dalla fase di pianificazione degli investimenti, dato che è in tale fase che vengono compiute le scelte strategiche. Si dovrà mettere le Amministrazioni in grado di valutare, verificare e dimostrare le giustificazioni economiche dei loro investimenti: dunque la raccomandazione andrà accompagnata con opportune indicazioni e criteri di riferimento. Tali criteri di riferimento potranno essere estratti dalla metodologia generale del **Value Management** che è un approccio strutturato alla conduzione dei progetti, finalizzato al controllo degli obiettivi, all'eliminazione degli sprechi e alla massima efficacia delle scelte adottate.³³

³⁰ "Indagine conoscitiva sul software a sorgente aperto nella PA", <http://www.innovazione.gov.it>.

³¹ Sono le applicazioni sviluppate ad hoc da un fornitore per una specifica esigenza di una o più amministrazioni o clienti.

³² La PA acquisisce il diritto di utilizzare un prodotto software esistente. Tale acquisizione è regolata da opportune licenze che indicano i vincoli e i diritti che sono garantiti al titolare della licenza stessa.

³³ "Indagine conoscitiva sul software a sorgente aperto nella PA", <http://www.innovazione.gov.it>.

Le attività del Value Management si svolgono principalmente nelle prime fasi del progetto (studio di fattibilità), ma proseguono attraverso review anche nelle fasi successive (analisi, implementazione). Esse consistono essenzialmente nel:

1. identificare e valutare i mezzi utilizzati per soddisfare i requisiti e gli obiettivi del progetto
2. verificare che le decisioni prese nell'arco del progetto siano le più efficaci a raggiungere gli scopi prefissati
3. in corso d'opera, investigare e verificare la fattibilità di modifiche, valutando i possibili risparmi
4. verificare in definitiva che le risorse impiegate nel progetto vengano spese ove forniscono in cambio il massimo volume.

Applicare i metodi di Value Management alla problematica della scelta tra software OS e software proprietario permette di scegliere tra i due modelli non soltanto sulla base del semplice confronto tra il costo dell'acquisto iniziale, ma in modo strutturato. Oltre ai costi visibili delle due opzioni, di deve tener conto anche del cosiddetto **lock-in** cioè dei costi di uscita da una determinata tecnologia (migrazioni dati e applicazioni, fermo attività, nuova formazione ecc.).

In sintesi, l'adozione di software OS porta normalmente ad un risparmio iniziale in termini di costi per le licenze. Un confronto economico corretto deve però essere compiuto non solo sulla spesa iniziale ma tra il TCO delle soluzioni OS ed il TCO delle soluzioni proprietarie. Oltre al costo delle licenze, nel TCO confluiscono le spese dei servizi di supporto, della formazione, i costi di migrazione, d'installazione e di gestione. Le linee guida del governo inglese evidenziano molto pragmaticamente il Value for Money come criterio di scelta per il software OS.³⁴

La spesa delle PA italiane in software, nel 2003 si può stimare in 816 milioni di euro, in diminuzione del 6% rispetto all'anno precedente. Di questi, il 58% della spesa si è concentrata nello sviluppo, manutenzione e gestione di programmi custom per una specifica amministrazione. Il rimanente 42% è stato utilizzato per l'acquisizione, manutenzione o leasing di licenze di pacchetti.³⁵ Rispetto ai dati riportati dalla commissione Meo, dati che si riferivano al 2001, è cresciuta l'incidenza percentuale della spesa relativa al software venduto su licenza (dal 39% al 42%), mentre è diminuita la componente relativa al software sviluppato ad hoc (dal 61% al 58%). Tuttavia l'incidenza sul totale della spesa del software ad hoc resta ancora maggioritaria. Ciò conferma e rafforza la necessità di considerare alternative al software proprietario venduto su licenza ed al software sviluppato ad hoc.

11. La situazione e le iniziative in Europa.

³⁴ <http://tecnoteca.it>.

³⁵ "Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -", <http://cnipa.gov.it>.

Lo studio IDA (Interchange of Data between Administrations) guidato dalla Commissione Europea fece il primo punto della situazione sull'uso e sulle direttive di adozione del software OS da parte delle PA dei Paesi europei. Nel 2001 l'uso di software OS si concentrava in gran parte nel campo dei server. In particolare si registrava un ampio uso del web server Apache e del sistema operativo Linux, mentre l'uso di programmi OS in ambiente desktop risultava invece molto limitato. Nei casi di adozione di soluzioni OS, le caratteristiche percepite come determinanti per la scelta da parte dei manager IT del settore pubblico consistevano nell'interoperabilità, la sicurezza, il rispetto degli standard e la funzionalità. La caratteristica del basso costo, invece, non emergeva dall'analisi.³⁶

Lo studio forniva una serie di indicazioni sulle possibili iniziative governative in favore dell'adozione di software OS. Se da un lato il supporto diretto attraverso finanziamenti pubblici, veniva indicato come una iniziativa controversa, veniva fortemente consigliato il supporto indiretto. Esso consisterebbe nella promozione di standard aperti, strettamente legati al movimento OS, nel finanziamento indiretto degli sviluppatori attraverso le sovvenzioni alla ricerca scientifica.

L'azione governativa dovrebbe concentrarsi nel limitare gli effetti negativi delle leggi riguardanti la proprietà intellettuale, andrebbe soprattutto evitata l'introduzione di brevetti sul software che andrebbero a danneggiare il tessuto delle piccole imprese ed in particolare, il mondo dell'OS ponendo barriere spesso insormontabili agli sviluppatori. Un sostegno indiretto all'OS è rappresentato anche da quelle iniziative tese a rinforzare gli effetti delle leggi Antitrust in presenza di casi di eccessiva dominanza. Nel 2002, la Commissione Europea ha prodotto il report "Pooling OSS" che trattava dei risparmi ottenibili condividendo il software OS. Lo studio raccomandava di creare un sistema ove il software sviluppato per il settore pubblico potesse essere raccolto su base di donazione per un successivo riutilizzo. Nel agosto 2003 fu attivata l'iniziativa denominata "Encouraging good practice in the use of OSS in the Public Administrations".

Tale iniziativa comportò principalmente lo sviluppo di Centri di competenza nazionali e regionali per facilitare lo scambio di informazioni sulle opportunità e i rischi connessi all'OS.³⁷ Con riferimento ai Centri più significativi, a livello di istituzioni europee è da citare innanzitutto l'Open Source Observatory (OSO), che ha come scopo raccogliere e condividere risorse OS provenienti dalle Amministrazioni europee, incoraggiare la diffusione e l'uso di best practice in Europa. Tra le sezioni più significative del sito dell'OSO³⁸ si cita in particolare:

- la sezione dedicata ai casi di studio

³⁶ <http://www.tecnoteca.it>.

³⁷ "Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -", <http://www.cnipa.gov.it>.

³⁸ <http://www.ec.europa.eu/idabc/en/chapter/452>.

- la sezione “risorse”, ove si può trovare un elenco di centri e organizzazioni
- le news sulle attività dei governi europei ed extraeuropei
- un documento sulle politiche OS in Europa ed extra UE

Il programma IDA è stato sostituito dal IDABC (Interoperable Delivery of European eGov Services to Public Administrations, Business and Citizens). Questo programma sfrutta le opportunità offerte dall’ICT, utilizzando lo stato dell’arte, sviluppando soluzioni e servizi comuni e, in fine, fornendo una piattaforma per lo scambio delle good practice tra le PA europee.³⁹ IDABC contribuisce agli obiettivi dell’ e-Europe di modernizzare il settore pubblico dell’ EU.

12. La politica sull’Open source in Francia

Il governo Francese ha considerato l’uso di soluzioni OS e le nuove tecnologie in alcune tematiche di interesse nazionale, quali ambiente, trasporti, sanità, tecnologie per i disabili, formazione on line. Per analizzare queste tematiche furono costituite una Commissione interministeriale di indirizzo per le società che operano nel mondo delle tecnologie (CISI) e una Commissione ministeriale il cui obiettivo era fornire indicazioni relativamente alla modernizzazione dell’Amministrazione statale (CIRE).

Alla fine del 1998 le Istituzioni pubbliche francesi cominciarono ad adottare il software OS nei loro sistemi informativi, all’interno del Ministero della Difesa, della Giustizia, dell’Economia, Finanza e Industria.⁴⁰ L’ADAE (Agence pour le développement électronique) è un servizio interministeriale creato il 21 febbraio 2003 e collocato presso l’ufficio del Primo Ministro; ha preso il posto dell’ATICA, che a suo tempo aveva pubblicato un documento con lo scopo di proporre alle Amministrazioni un metodo di scelta e di uso delle licenze di software libero in relazione alle due situazioni nelle quali le stesse possono trovarsi:

- acquisto (a titolo oneroso o gratuito) di software e componenti
- sviluppo di software sviluppato da o per conto delle amministrazioni.

Nel corso del programma di amministrazione elettronica 2004/2007 denominato ADELE⁴¹ sono previsti tre progetti attinenti a tematiche Open source:

- messa in opera di software libero e strumenti di sviluppo collaborativo
- piattaforma tecnica per lo sviluppo collaborativo: centri di risorse tecniche
- migrazioni di posti di lavoro.

³⁹ <http://www.ec.europa.eu/idabc>.

⁴⁰ “Indagine conoscitiva sul software a sorgente aperto nella PA”, <http://www.innovazione.gov.it>.

⁴¹ <http://www.adele.gouv.fr>.

L'ADAE mantiene inoltre un repertorio per il riuso del software e dei progetti sviluppati da varie amministrazioni dello Stato francese in open source.⁴²

La Corte di Cassazione francese ha iniziato la sua nuova sessione con un nuovissimo sito basato su Linux e su software Open source. Il nuovo sito, inaugurato il 6 settembre 2006, conferma l'entusiasmo crescente del settore pubblico francese per le soluzioni Open source. Il sito della Corte di Cassazione è stato sviluppato in linguaggio PHP, oltre 8000 pagine web degli archivi della Corte sono state convertite nella nuova struttura che è adesso più flessibile e facile da gestire.⁴³

13. La politica sull'Open source in Germania.

Il Governo federale tedesco considera il software Open source come uno dei modelli per lo sviluppo della società dell'informazione e ha previsto una serie di iniziative indirizzate a chiarire i vantaggi e gli svantaggi del software OS. Tra queste:

- Istruzioni pratiche alle imprese
- Formazione di un "competence center" per il software OS, con un forum permanente di discussione (BerliOS)
- Supporto di un prodotto per la crittografia, rispondendo ad una specifica esigenza del Governo (GNuPG)
- Indicazioni sul processo di migrazione da software proprietario a software OS.

Il Governo tedesco ha deciso inoltre di finanziare lo sviluppo di una soluzione desktop OS per le PA su piattaforma Linux con le motivazioni di ridurre i costi, aumentare la stabilità e la sicurezza, limitare la dipendenza da soluzioni software e prodotti proprietari.⁴⁴

In particolare, venne accolta con un certo entusiasmo dalla comunità OS la notizia che il consiglio comunale di Monaco di Baviera approvò nel 2003 un piano per il passaggio graduale da Windows a Linux (progetto LiMux – Linux in Munich) per i propri sistemi informatici. Il consiglio decise per Linux nonostante gli ampi sconti proposti da Microsoft sui propri software. In ballo vi erano, evidentemente, quelle considerazioni che ormai da tempo riescono a far breccia in molte amministrazioni pubbliche e che vanno al di là della diatriba sul costo di Windows w sul costo effettivo di Linux.⁴⁵ Ci sono considerazioni sull'accessibilità dei documenti, sulla sicurezza e

⁴² "Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -", <http://www.cnipa.gov.it>.

⁴³ "FR: Court of Cassation turns to Open Source", copyright European Communities 2006, <http://ec.europa.eu/idabc/en/document/5834/469>.

⁴⁴ "Indagine conoscitiva sul software a sorgente aperto nella PA", <http://www.innovazione.gov.it>.

⁴⁵ "In Baviera vince l'OS", Punto informatico, anno VIII, n. 1842 del 28/5/2003, <http://www.punto-informatico.it>.

probabilmente ancora più rilevanti per le PA, la possibilità di verificare il codice Linux.

Dopo un travaglio durato quasi due anni, il Comune di Monaco ha finalmente dato alla luce una propria versione di Linux che verrà installata su numerosi server e su 14 mila computer desktop e 16 mila portatili. Non manca la suite per ufficio OpenOffice (di cui ci occuperemo in una apposita sezione) che sui desktop “convertiti” avrà il compito di sostituire Ms Office. Il progetto Linux si è occupato, tra le altre cose, di fare o migliorare la traduzione in tedesco di tutti i pacchetti software e della relativa documentazione, di redigere manuali e linee guida sull’uso di Linux e OpenOffice. I responsabili del progetto contano di completare la migrazione per la fine del 2008, una data entro cui Linux e OpenOffice dovrebbero girare sull’ 80% di tutti i Pc desktop dell’Amministrazione pubblica di Monaco.⁴⁶

L’attuazione del progetto Linux sta richiedendo molto più tempo del previsto, oltre ai problemi tecnici e di formazione del personale, a frenare il progetto tedesco è intervenuto anche il timore che Linux potesse infrangere certi brevetti, timore che la città bavarese ha dissipato commissionando ad uno Studio legale un’analisi dei rischi. Tra le altre città europee ad aver annunciato ambiziosi piani su Linux c’è Vienna, con cui il Comune di Monaco sta collaborando per armonizzare i relativi progetti.

14. Formati aperti e formati standard.

Un **formato aperto** può essere definito come la “modalità di rappresentazione dei dati in forma elettronica, deliberatamente resa pubblica, completamente documentata ed utilizzabile da chiunque”. In questo senso ad esempio, il formato utilizzato da Openoffice è un formato aperto in quanto:

- è una modalità di rappresentazione dei dati in forma elettronica
- è esaustivamente documentato ed utilizzabile da chiunque (i dati vengono rappresentati nativamente in XML⁴⁷ la cui struttura è definita in una DTD (document type definition), grammatica di una classe di documenti XML, pubblica).

Un formato è **standard** quando è definito da un ente di standardizzazione (es. HTML) o è di fatto condiviso da una comunità (es. PDF).

Un formato aperto deve poter essere implementato senza distinzioni da software proprietari, open source o liberi, ciascuno con le proprie modalità di licenza. A differenza dei formati aperti i formati proprietari sono controllati e definiti da interessi privati. La relazione tra formati aperti ed il software OS è spesso fonte di malintesi.⁴⁸ Molti software proprietari fanno largo uso di formati aperti ed il software OS può a volte usare formati proprietari (es.

⁴⁶ “Monaco partorisce il suo Linux”, Punto informatico, anno XI, n. 2616 del 29/9/2006, <http://www.punto-informatico.it>.

⁴⁷ Standard internazionale nato per gestire documenti in ambito internet, si è rivelato una potente tecnologia per l’adozione di formati aperti, è attualmente la migliore soluzione disponibile per perseguire la persistenza dell’accesso all’informazione rispetto al mutare delle tecnologie.

⁴⁸ <http://it.wikipedia.org>.

HTML gestito da Explorer oppure i file .doc gestiti da OpenOffice). L'obiettivo principale dei formati aperti è di garantire l'accesso ai dati nel lungo periodo senza incertezza presente e futura riguardo ai diritti legali o le specifiche tecniche.⁴⁹

Uno dei problemi più delicati che le PA si trovano ad affrontare è quello che concerne la conservazione e distribuzione delle informazioni. Tale problema investe sia la sfera dei rapporti che intercorrono tra diverse Amministrazioni (governement to governement - g to g), sia quelli che coinvolgono i cittadini (governement to citizen - g to c). Deve essere possibile a chiunque accedere ad uno specifico documento e/o informazione di una PA, senza dover necessariamente acquisire uno specifico strumento software proprietario.

La questione va al di là del garantire accesso libero alle informazioni.⁵⁰ Un documento creato con un pacchetto proprietario contiene informazioni che rimangono di proprietà dell'Amministrazione che lo ha generato. Deve quindi essere sempre possibile accedere alle informazioni contenute in quel documento, anche quando si decidesse di non utilizzare più il pacchetto proprietario originariamente usato per crearlo. E' quindi pieno interesse delle PA di poter disporre di programmi che facciano uso di standard aperti, che assicurano indipendenza dai fornitori alta interoperabilità e maggiore libertà di scelta per gli utenti. Inoltre i formati testo aperti standard comportano l'ulteriore beneficio della persistenza, caratteristica importante per la tutela del patrimonio informativo nel tempo a fronte del mutamento tecnologico⁵¹, pertanto le informazioni rappresentate con questo formato sono recuperabili anche molto tempo dopo la generazione senza necessità di pesanti riconversioni.

Presentando i lavori conclusivi del rapporto della Commissione ministeriale sul software OS nella PA, l'allora Ministro per l'Innovazione e le Tecnologie Stanca pose quindi come centrale la questione "dell'accessibilità dei documenti delle PA, che devono essere resi disponibili attraverso almeno un formato aperto consentendone così l'indipendenza da specifici pacchetti software di mercato e permettendo anche la loro conservazione nel tempo"⁵² Raccomandazioni poi sfociate nella stesura dell'art. 4 della Direttiva del 19/12/2003 "Sviluppo ed utilizzazione dei programmi informatici da parte della PA" (G. U. n. 31 del 7/2/2004).

15. Il formato Open Document Format (ODF).

Uno degli obiettivi dei formati aperti come Open Document è quello di garantire, come abbiamo visto, l'accesso a lungo termine ai dati senza barriere legali o tecniche, per questo motivo le amministrazioni pubbliche ed i Governi

⁴⁹ Esempi di formati aperti: TXT, RTF, JPEG, OGG.

⁵⁰ "Indagine conoscitiva sul software a sorgente aperto nella PA", <http://innovazione.gov.it>.

⁵¹ <http://www.tecnoteca.it>.

⁵² Comunicato Stampa del Dipartimento per l'Innovazione e le Tecnologie del 29/09/03.

sono diventati progressivamente consapevoli dei formati aperti come questioni che riguardano le politiche pubbliche.⁵³ Il formato Open Document (ODF), abbreviazione di OASIS Open Document Format for Office Applications, è un formato aperto per i file di documento, per il salvataggio e lo scambio degli stessi per la produttività d'ufficio, come documenti di testo, diagrammi e presentazioni. Questo standard è stato sviluppato dal Consorzio di industrie OASIS ed è impostato su una versione di XML creata originariamente per Open Office. Lo standard è stato sviluppato pubblicamente da varie organizzazioni ed è pubblicamente accessibile, può essere implementato da chiunque senza restrizioni.

Open Document nasce per fornire un'alternativa "aperta" a formati proprietari tra cui i famosi file .doc e .ppt usati da Ms Office, il formato può essere utilizzato gratuitamente da qualsiasi applicazione per l'ufficio senza nessuna licenza. Una caratteristica che svincola quindi le aziende pubbliche e private dalle tecnologie proprietarie e dà loro garanzia che tutti i propri documenti potranno essere sempre aperti e modificati.⁵⁴

Secondo il datasheet Open Document di OASIS, "il Ministero della Difesa di Singapore, il Ministero delle Finanze francese ed il suo Ministero dell'Economia, Finanza e Industria, il Ministero della Salute brasiliano, la città di Monaco, il Consiglio municipale di Bristol e la città di Vienna, stanno tutte adottando in questo periodo applicazioni che supportano questo formato". Al termine di un processo durato due anni il formato dei documenti Open Document (ODF) ha finalmente guadagnato il riconoscimento ufficiale dell'International Organization for Standardization (ISO), questo infatti, con una recente votazione ne ha fatto un proprio standard.

La certificazione di ODF da parte di ISO/IEC (International Engineering Consortium) è stata fortemente voluta dalla Commissione Europea che lo ha inoltre raccomandato come base per i formati di file standard e per lo scambio di documenti. E' stata infatti quest'ultima nel maggio del 2004 ad esortare OASIS⁵⁵ a presentare la specifica ODF all'ISO.⁵⁶ L'ISO ha approvato e accettato Open Document il 1 maggio 2006 (ISO 26300), un riconoscimento davvero importante se si pensa che l'aderenza agli standard ISO è richiesta da Amministrazioni pubbliche e grandi aziende internazionali.⁵⁷

16. Il caso Open Office.org

⁵³ <http://it.wikipedia.org>.

⁵⁴ "Open Document consacrato dall'ISO", <http://www.punto-informatico.it>.

⁵⁵ OASIS è il Consorzio internazionale in seno al quale è stata sviluppata e standardizzata la prima versione ufficiale di ODF for Office Applications, una specifica ampiamente basata sul formato XML.

⁵⁶ "Open Document consacrato dall'ISO", <http://www.punto-informatico.it>.

⁵⁷ "ODF di Open Office approvato ISO 26300", di Samuel Zilli, del 4/5/06, <http://www.azpoint.net>.

A metà degli anni '80 lo studente tedesco Marco Borries cominciò lo sviluppo di un software per l'ufficio, più tardi conosciuto come Star Office, e fondò l'azienda Star Division. Spinta da motivazioni strategiche e commerciali, la Sun Microsystem, acquisì sul finire degli anni '90 la Star Division. Fu ben presto evidente ai manager di Sun che l'impresa di contendere significative fette di mercato a Ms Office fosse ben più difficile del previsto e così il progetto Star Office venne accantonato. Questo fu tuttavia rilanciato più tardi attraverso la pubblicazione del codice sorgente del prodotto e l'affidamento dello stesso alla comunità OS, con il contributo degli sviluppatori già in forza alla divisione Star Office di Sun.⁵⁸

Il progetto Open Office.org (il suffisso .org è stato inserito a causa di una disputa sul marchio) fu fondato da Sun il 13 ottobre 2000 per continuare lo sviluppo internazionale di una Suite da ufficio che fosse in grado di funzionare su tutte le piattaforme più importanti. Da quel momento si è creata una comunità internazionale che ha sviluppato, integrato e migliorato quella generosa donazione iniziale, fino a giungere alla realizzazione della prima vera suite Open source per ufficio che utilizza il formato ODF: Open Office.org 1.0.⁵⁹ Oggi il progetto conta migliaia di sviluppatori che contribuiscono in forme e misure diverse a supportare un prodotto che conta milioni di installazioni ed è tradotto in 91 lingue. Tra le molteplici ragioni di questo successo, vi è certamente il modello di sviluppo adottato in grado di produrre ricadute positive sull'economicità ed efficienza del prodotto, lasciandolo nel contempo libero da qualsiasi vincolo sui formati utilizzati per la manipolazione e memorizzazione dei dati. Venerdì 13 ottobre 2006 in occasione del 6° anniversario è stata rilasciata la versione 2.0.4.

17. L'espansione di ODF e Open Office.org

Secondo un rapporto realizzato da Ramboll Management per l'Associazione dei Providers OS in Danimarca (OSL), l'intero settore Pubblico danese potrebbe risparmiare all'incirca 73,7 milioni di euro con il passaggio all'utilizzo di ODF. Prima dell'estate 2006, il Parlamento danese ha deciso di introdurre Open standards nella sua Amministrazione Pubblica. OSL ha commissionato un rapporto a Ramboll mirato alla stima dei probabili costi di tre differenti scenari in caso di passaggio agli Open standards. I tre scenari in questione erano i seguenti:

1. Uso di Ms Office e del formato Open XML (proprietario) in relazione al lancio di Ms Office 2007
2. Migrazione allo standard ODF con il passaggio simultaneo alla suite da ufficio OpenOffice
3. Introdurre ODF come un plug-in all'interno di Ms Office.

I costi stimati per il primo scenario risultavano essere 51 milioni di euro. Per il secondo, il costo si aggirava sui 34 milioni di euro, con un

⁵⁸ “Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto -”.

⁵⁹ “Retrosceca storico”, <http://it.openoffice.org>.

risparmio di circa 16,8 milioni di euro, su 5 anni, per la sola Amministrazione Centrale e di circa 73.7 milioni per l'intera Amministrazione Pubblica. Il terzo scenario si rivelava marginalmente più costoso del primo, a causa dei maggiori costi per la conversione ed il supporto.⁶⁰

Il rapporto di Ramboll Management rappresenta un contributo importante nel momento in cui il settore pubblico sta prendendo la decisione di introdurre gli Open Standards. La scelta tra l'Open XML di Microsoft ed il formato ODF è molto importante perché il primo è collegato ad una specifica azienda, Microsoft. Non è auspicabile mettere nelle mani di una singola azienda gli standard pubblici di IT.

In Belgio, il Governo federale ha dato il via libera all'uso di Open Document in tutti gli uffici della PA. Il formato aperto ha così conquistato un'importante roccaforte all'interno dell'UE. L'implementazione di ODF inizierà dal settembre 2008, quando tutta la PA diventerà supporto di base per i sistemi informatici nazionali. I portavoce dell'amministrazione belga hanno affermato che "bisogna evitare di dipendere da qualsiasi fornitore di software perché ormai la comunicazione istituzionale passa soprattutto attraverso la posta elettronica e l'invio di allegati digitali, un flusso di dati straordinario che spinge ad adottare gli standard aperti".⁶¹

Il cammino di OpenDocument verso l'adozione internazionale ha subito un'importante accelerazione quando è stato reso noto un rapporto sull'adozione dei formati liberi voluto dal Primo Ministro francese Dominique de Villepin. Il parlamentare Bernard Carayon non solo delinea i vantaggi che i cittadini francesi otterrebbero se la PA adottasse OpenDocument ma suggerisce al governo di farsi portavoce di un'iniziativa europea per spingere tutti partners dell'Unione ad adottare sistematicamente i formati aperti, ODF in primis. Carayon sottolinea come ODF sia stato consacrato lo scorso maggio quale standard dall'ente internazionale ISO, un passaggio che "garantisce perennemente" l'accessibilità di documenti realizzati con questo formato, consentendone "l'uso senza rischi da parte dei soggetti economici ed enti pubblici".⁶²

I primi passi da fare consistono nel rendere obbligatorio nella PA francese l'utilizzo di ODF e nel chiedere all'Unione Europea di realizzare in ODF qualsiasi documento venga scambiato e pubblicato a livello istituzionale comunitario. Secondo il rapporto, infatti, solo l'adozione di formati aperti e interoperabili pone "le condizioni dello sviluppo economico europeo per quanto riguarda le tecnologie dell'informazione". In questo senso è necessario, viene sottolineato, che "l'interoperabilità diventi un requisito legale fondamentale".

⁶⁰ "DK: Danish reports forecasts major savings from a danish public sector switch to Odf", OS News del 14/9/2006, <http://ec.europa.eu/idabc/en/document/5830/469>.

⁶¹ "Il Belgio adotta il formato Open Document", Punto informatico, anno XI, n. 2569 di mercoledì 28/9/06, <http://www.punto-informatico.it>

⁶² "Parigi:L'Europa marci verso Open Document", Punto informatico, anno XI n. 2624 di venerdì 6/10/06, <http://www.punto-informatico.it>

Per quanto riguarda la situazione extra europea, all'inizio del 2005, Eric Kriss, Segretario dell'Amministrazione e delle Finanze in Massachusetts, è stato il primo membro di un governo di uno Stato degli Stati Uniti a collegare i formati aperti ad uno scopo di politiche pubbliche: "E' obbligo prioritario del sistema democratico Americano che non possiamo avere i nostri documenti pubblici vincolati in un qualche tipo di formato proprietario, magari non visualizzabile in futuro o soggetto ad un sistema di licenza proprietario che ne restringe l'accesso".

A settembre 2005, il Massachusetts è diventato il primo Stato ad assumere formalmente il formato OpenDocument per i propri archivi pubblici e, allo stesso tempo, rifiutare il formato proprietario Microsoft XML (ora chiamato Microsoft Office Open XML).⁶³

18. Considerazioni conclusive.

Ben venga quindi l'Open source all'interno della nostra PA, numerosi sono i vantaggi che se ne possono trarre nel breve periodo. L'inclusione di questa tipologia di offerta all'interno delle soluzioni tecniche tra cui la PA può scegliere contribuisce infatti ad ampliare la gamma delle opportunità e delle possibilità in un quadro di economicità, equilibrio, pluralismo e aperta competizione. Tra i principali aspetti analizzati che spingono a favore della scelta per questa tipologia di software possiamo ricordare le esigenze di indipendenza della nostra Amministrazione, esigenze che vengono soddisfatte appieno attraverso l'utilizzo dell'OS che svincola dal restare legati (per il supporto del software ad esempio) ad una singola azienda. Il centro della questione non è solo, come potrebbe sembrare, la gratuità né l'economicità di questa tipologia di software, quanto la stabilità, la trasparenza e la sicurezza che il modello Open source può offrire alla PA. Attraverso l'apertura dei sorgenti si può ad esempio verificare all'interno dell'applicativo l'esistenza di banchi o **back doors** utilizzati a discapito della tutela della privacy dei cittadini.

La visibilità dei sorgenti permette inoltre di riadattare il software utilizzato da una determinata Amministrazione a beneficio di un'altra, attraverso la tecnica del riuso. Per quanto riguarda l'aspetto economico, come abbiamo visto, una corretta analisi e comparazione tra software Open source e software proprietario va fatta prendendo in considerazione non solo la spesa iniziale dell'acquisto (nettamente in favore del sw OS) ma utilizzando le metodologie del **Value Management** che ci portano a considerare altri fattori, come ad esempio il cosiddetto **lock-in**, cioè i costi di uscita da una determinata tecnologia (migrazione dei dati e applicazioni, fermo attività, nuova formazione del personale). A mio modesto parere anche in questo caso è da preferire il passaggio al software OS soprattutto se prendiamo in considerazione le soluzioni desktop, come ad esempio **Linux** che utilizza ormai interfacce grafiche particolarmente funzionali, utilizzabili da chiunque senza particolari problemi di aggiornamento.

⁶³ <http://it.wikipedia.org>.

Inoltre, l'utilizzo di **OpenOffice.org** (e del formato aperto da esso supportato, ODF) in alternativa a **Ms Office** non apporta particolari problemi di adattamento e formazione del personale essendo una suite da ufficio che ricalca in pieno le funzionalità della soluzione offerta da Microsoft, fatto che ne sta provocando l'espansione continua in tutte le pubbliche amministrazioni europee e non solo. L'Unione Europea è infatti proiettata verso una politica di netto favore sia per i formati "aperti" di cui auspica il diffuso utilizzo per lo scambio dei documenti, grazie anche alla recente certificazione ISO ricevuta da ODF, sia per il software OS (l'Osservatorio europeo sull'OS ne è un esempio). Vorrei, per concludere, riproporre ed associarmi al pensiero del Segretario dell'Amministrazione e delle Finanze del Massachusetts Eric Kriss cioè che è obbligo del sistema democratico non avere i documenti pubblici vincolati in qualche tipo di formato proprietario (ad esempio .doc), magari non visualizzabile in futuro o soggetto ad un sistema di licenza proprietario che ne restringe l'accesso.

La stesura finale della presente ricerca, nella sua formulazione originaria, è stata effettuata utilizzando Openoffice.org (versione 2.0.4) scaricabile gratuitamente dal sito <http://it.openoffice.org>.

CAPITOLO III

NICOLÒ ROBERTO PERDICARO

INTEGRAZIONE DI BANCHE DI DATI IN AMBIENTE SOCIO SANITARIO. VALUTAZIONE DI COSTI E DI BENEFICI.

SOMMARIO: 1. Premessa. – 2. Open source e Free software, definizioni e differenze. – 3. Open Source e diritto d'autore. – 4. Le licenze di software libero, la GPL. – 5. Open source e P.A. - Quadro storico di riferimento. – 6. La direttiva sull'Open Source. – 7. L'Osservatorio Open source presso il CNIPA. – 8. La situazione nelle P.A.L. – 9. I vantaggi per la P.A. – 10. La questione economica - Il Value Management. – 11. La situazione e le iniziative in Europa. – 12. La direttiva sull'Open Source in Francia. 13 – La direttiva sull'Open Source in Germania. – 14. Formati aperti e formati standard. – 15. Il formato Open Document Format (ODF). - 16. Il caso Open Office.org – 17. L'espansione di ODF e Open Office.org. – 18. Considerazioni conclusive.

1. Premessa

Quando per diversi motivi si parla della nostra personale salute, frequentemente ci viene richiesto da diversi operatori socio-sanitari: medici di base, infermieri, dentisti, istruttori di educazione fisica, tecnici di laboratori di analisi, dietologi, oculisti, di rappresentare il nostro stato di salute evidenziando, di volta in volta, gli aspetti che si ritengono utili alle finalità dell'anamnesi e della seguente terapia.

Si costituiscono così, diverse cartelle cliniche contenenti informazioni sul nostro stato di salute. A volte queste informazioni si completano a vicenda, ma il più delle volte esse sono ridondanti, cioè sono ripetitive.

Con la costituzione di questa massa di informazioni sul nostro stato di salute si aprono due scenari ricchi di aspetti che questo mio lavoro cercherà di analizzare nelle sue macroscopiche tematiche: il primo scenario è quello derivante da una considerazione: quando veramente servono, e speriamo che non servano mai, al medico del pronto soccorso che deve conoscere il paziente ricoverato urgentemente, queste informazioni sono irreperibili, frammentate e difficilmente verificabili in un lasso di tempo accettabile.

L'altro scenario meno importante, ma da un altro punto di vista, ugualmente preoccupante è derivato dal fatto che non sappiamo con certezza come questi dati sulla nostra salute sono conservati, da chi sono conservati e che uso se ne fa.

Partendo da questa premessa ho voluto per prima cosa indagare la situazione più generale dell'utilizzo dell'ICT (Information and Communication Technology), in altri paesi e quindi in Italia, illustrare la realtà dell'organizzazione socio-sanitaria prendendo a riferimento due regioni, Toscana e Umbria, oltre ad iniziative locali, per valutare la possibilità di rendere reale un modello organizzativo finalizzato a rendere condivise le varie

banche dati che, seppur costituite in maniera frammentata, possono organicamente confluire nella cosiddetta “cartella sanitaria digitale”.

Infine illustrerò un metodo di valutazione di costi e benefici utile a valutare, successivamente alla realizzazione, un progetto innovativo di integrazione di dati in ambiente socio-sanitario.

2. La gestione dei dati in ambiente sanitario e l'utilizzo dell'Information and Communication Technology (ICT) in sanità.

Alcuni paesi europei e nel mondo (Inghilterra, Danimarca, Canada, Australia), caratterizzati da una elevata presenza del settore pubblico e da una forte autonomia regionale, hanno sviluppato progetti per l'utilizzo dell'ICT nel sistema sanitario.

Questi paesi hanno coscienza che la trasformazione info-telematica del sistema sanitario deve essere attentamente pianificata e verificata se si vogliono trarre da questi sacrifici economici dovuti alla trasformazione organizzativa quei benefici ricercati in termini di qualità dell'assistenza, soddisfazione dell'utenza, efficacia complessiva dell'azione e risparmi economici.

Pertanto la strategia adottata da questi Paesi è stata quella di creare, a livello centrale, un organismo tecnico formato da elementi decisori e da tecnici altamente qualificati, a livello intermedio, formato dagli Enti locali e territoriali ed infine a livello periferico formato dalle Aziende sanitarie, sindacati di categoria, associazioni, industrie e cittadini.

3. La situazione in Italia.

Il 2003 è stato un anno importante per la definizione di un piano nazionale di sviluppo di una Società dell'informazione finalizzata a migliorare la qualità della vita. Con il protocollo d'intesa firmato il 27 marzo 2003, tra il Ministro per l'Innovazione e le tecnologie, Lucio Stanca, e il Ministro della salute, Girolamo Sirchia, il Governo sancisce lo sviluppo di un modello di Società dell'Informazione finalizzato anche a migliorare la qualità della vita e a prevenire esclusioni di natura sociale ed economica.

Successivamente un altro apporto alle politiche di una “sanità in rete” è contenuta nel piano *eEurope 2005*, dell'Unione Europea. Il piano *eEurope 2005* sviluppato secondo logiche di inclusione e di protezione dell'informazione sanitaria, individua come obiettivi prioritari per gli stati Membri:

- lo sviluppo di una tessera sanitaria elettronica;
- la realizzazione di reti di informazione sanitaria;
- servizi affidabili ed efficienti di telemedicina e teledidattica.

Ma vediamo, in sintesi, lo stato di realizzazione dei questi progetti.

In Italia, la legge 27 dicembre 2002, n. 289 prevede “*che al fine di potenziare il processo di attivazione del monitoraggio delle prescrizioni mediche, farmaceutiche, specialistiche ed ospedaliere e al fine di contenere la spesa sanitaria nonché di accelerare l’informatizzazione del sistema sanitario e dei relativi rapporti con i cittadini, le pubbliche amministrazioni*” stabiliscano le modalità per l’utilizzo della carta sanitaria riconosciuta come elemento strategico per l’attuazione del Sistema Informativo Sanitario Nazionale (NSIS), in quanto strumento per l’identificazione certa dei cittadini e di accesso sicuro alle informazioni sanitarie individuali.

Con questi presupposti il Governo nel 2003 dà il via ad un piano di azione che prevede per la Sanità in rete del nostro Paese:

1. diffusione della Carta sanitaria per l’accesso ai servizi telematici del Servizio sanitario nazionale e all’attuazione dell’Electronic Health Record, parte integrante del NSIS;
2. sviluppo della telemedicina e della teledidattica in sanità, con particolare riferimento a:
 - all’attivazione di reti telematiche, in particolare nell’area oncologica, in grado di rendere sistematica la cooperazione clinica e diagnostica dei Centri di Eccellenza;
 - all’attuazione del progetto per l’Integrazione e la Promozione degli Ospedali e Centri di cura italiani nel Mondo (IPOCM);
 - alla sperimentazione di servizi di teleconsulto e telediagnosi applicati alla rete sanitaria delle isole minori;
3. sviluppo di infrastrutture a larga banda e sicure per il collegamento di medici di base e delle strutture ospedaliere in ambito nazionale;
4. progetti di e-government e di e-procurement riferiti nell’ambito sanitario;
5. promozione di azioni per favorire l’accesso alle informazioni e ai servizi sanitari da parte dei disabili e degli anziani;
6. iniziative in ambito internazionale e comunitario sulla sanità in rete;
7. progetti di ricerca finalizzati all’utilizzo dell’ICT in ambito sanitario.

A livello regionale e locale, vi sono diversi progetti che perseguono la realizzazione di queste finalità. Di seguito mi soffermo su 2 progetti di altrettante regioni, Toscana e Umbria e su alcuni progetti locali.

4. Gli obiettivi del sistema informativo regionale toscano in ambito sanitario.

La Regione Toscana ha emanato nel 2003 un piano di sviluppo tendente a stimolare l’utilizzo degli strumenti dell’ICT anche nella sanità finalizzati a sviluppare le conoscenze dei rischi per la salute, le relazioni tra i diversi settori operativi delle aziende sanitarie, l’integrazione tra i diversi settori che devono garantire le prestazioni ed infine, il miglioramento delle modalità di fruizione dei servizi da parte dell’utente.

L’esperienza condotta dalla Regione Toscana negli anni precedenti ha evidenziato la rigidità della struttura organizzativa della Sanità pubblica a

produrre una pianificazione degli interventi nel settore tecnologico. Questo fatto è dovuto a diversi fattori come: 1) la difficoltà ad aggiornare modelli di lavoro per integrarli nella società dell'informazione, 2) alla continua innovazione che a volte non trova pratici riscontri, 3) alla scarsa propensione ad adottare una razionale catena di analisi/decisione/produzione/monitoraggio (ciclo di Deming).

Tutti questi fattori spingono le aziende che si occupano di e-sanità a rallentare l'investimento, già marginale, nel settore, interpretato spesso come un investimento a "bassa redditività".

Altro limite nella diffusione dell'ICT è rappresentato dalla distinzione rigida tra strutture organizzative dei sistemi informatici e quelle dei sistemi tecnologici.

Tale distinzione è provocata dal profilo delle diverse competenze professionali che tendono a caratterizzarle mostrando una generale scarsa flessibilità organizzativa che sarebbe tornata utile nella visione strategica dello sviluppo degli strumenti di conoscenza interno alle Aziende sanitarie.

La Giunta regionale toscana per ovviare a queste difficoltà ha attuato le seguenti linee di intervento:

- qualificazione dei flussi informativi regionali a supporto delle decisioni a livello regionale, aziendale e interaziendale;
- definizione di standard aziendali per realizzare un sistema di relazioni operative ed informative tra i soggetti coinvolti nei processi di erogazione dei servizi e delle prestazioni;
- definizione di standard di comune gestione dell'informazione tra le aziende sanitarie e gli altri soggetti del sistema sanitario in modo da consentire : a) ai fruitori dell'informazione, una condivisione di dati generali e/o specifici e b) come fornitori di informazioni, un accesso omogeneo al sistema informativo regionale, nazionale e per ambiti interaziendali;
- fruibilità del patrimonio informativo ovunque localizzato nel sistema sanitario, ma soprattutto quello presente a livello regionale.

Purtroppo la Regione Toscana commette, a mio avviso, un errore di strategia quando al fine di realizzare il proprio piano di sviluppo, lascia libere le ASL di provvedere direttamente alla implementazione di un piano complessivo di sviluppo ed adeguamento della propria struttura informatica ed organizzativa risolvendosi di ricoprire un ruolo di ente erogatore di finanziamenti senza attività di progettazione del piano e controllo dei risultati.

5. Sviluppo dei sistemi informatici nella sanità dell'Umbria.

La Regione Umbria ha dichiarato nel 2003 di aver compiuto un profondo processo di innovazione dell'organizzazione e degli strumenti tecnologici nelle Aziende sanitarie della regione.

Le azioni intraprese dalla Regione Umbria sono state finalizzate a migliorare l'efficienza operativa interna delle singole ASL e ad omogeneizzare lo sviluppo dei sistemi informativi in coerenza con le esigenze

di interoperabilità tra le stesse. Ciò è avvenuto sia sul piano delle infrastrutture che su quello dell'organizzazione.

In questi anni la regione Umbria si propone quindi di realizzare, attraverso la promozione dei servizi, dei rapporti con i cittadini utilizzatori, la comunicazione tra i diversi livelli del sistema e il miglioramento dell'efficacia e dell'efficienza dei processi interni e della gestione del sistema sanitario regionale.

Il modello concettuale adottato dalla Regione Umbria considera gli aspetti organizzativi e tecnologici come un insieme unico dove le soluzioni applicative del sistema informativo siano modulate sulle specificità organizzative e caratterizzate da un alto livello di flessibilità per adeguarsi alle esigenze di cambiamento che si dovessero verificare nel tempo.

6. Le caratteristiche del modello organizzativo.

Due sono le principali caratteristiche: la riorganizzazione delle funzioni tecnico-amministrative e l'autonomia tecnico-gestionale delle ASL.

La prima caratteristica è improntata sulla progressiva unificazione delle funzioni amministrative comuni alle varie ASL e Aziende Ospedaliere. Queste funzioni amministrative sono riferibili alla : 1) gestione amministrativa del personale, 2) acquisizione di beni e servizi, 3) gestione del patrimonio e delle tecnologie, 4) gestione del sistema informativo.

La seconda caratteristica è incentrata sulla capacità della struttura di sfruttare l'opportunità del risparmio sulle risorse economiche e umane per potenziare quei servizi più vicini alle esigenze dei cittadini – utenti, come ad esempio: 1) promozione e diffusione dell'informazione sui servizi erogati perché il cittadino possa assumere decisioni consapevoli sulle diverse possibilità di cura di sé stesso, 2) semplificazione dell'accesso dei cittadini – utenti alle visite ambulatoriali e agli accertamenti specialistici, 3) alla comunicazione dei referti in maniera digitale che presuppone l'attivazione di modalità di riconoscimento sicure, 4) sviluppo di modalità di interscambio dell'informazioni cliniche tra i vari soggetti operanti nel sistema sanitario.

7. L'architettura del sistema informativo.

Il modello di riferimento è assimilabile ad un sistema a rete. Rappresentabile come un'aggregazione di nodi operativi e centri di erogazione di servizi che cooperano per rispondere al bisogno di servizio dei cittadini e dei pazienti.

Questo modello richiede di risolvere le seguenti problematiche relative a :

- 1) sistemi di interfaccia con il cittadino – utente (sistemi di accesso, CNS, portale URP);
- 2) servizi di cooperazione degli attori del Sistema Sanitario Regionale (Infrastruttura di rete, interoperabilità, posta elettronica certificata, workflow, firma digitale);

3) sistemi Direzionali e di Controllo (Portale Direzionale).

8. Il progetto Gestione integrata dei Servizi Sociali e Socio sanitari (GE.NE.S.I)

La Provincia di Massa-Carrara ha approvato un progetto di e-government dal costo complessivo di quasi 2 milioni di euro con gli obiettivi di :

- Una migliore definizione delle finalità dei servizi e valutazione dei risultati
- Una integrazione fra Enti per l'ottimizzazione delle risorse
- Una facilitazione nella programmazione degli interventi sociali e socio-sanitari, attraverso la disponibilità di dati in forma standardizzata
- Una più facile analisi dei dati per il supporto alle decisioni

I servizi previsti dovranno facilitare:

- L'accesso
- L'accettazione
- La gestione
- La dimissione dei casi sociali e socio-sanitari

8a. Benefici di GE.NE.SI. per i cittadini.

- Accesso alla base dati delle strutture socio – sanitarie (sia attraverso un portale, che attraverso il contatto con assistenti sociali, che attraverso l'URP) accesso alle informazioni sui servizi ed iniziative sociali, sulle associazioni di Volontariato-Terzo Settore e sulle loro attività, su strutture erogatrici di prestazioni sociosanitarie;
- disponibilità di servizi telematici (download della modulistica necessaria per l'avvio di una procedura, possibilità di inoltro di richieste di servizi on line (non autenticata da certificati digitali ma solo da password consegnata via e-mail dopo riconoscimento del codice fiscale o codice sanitario)
- possibilità di accesso a servizi personalizzati previa verifica riconoscimento tramite certificato digitale (secondo le specifiche riportate nell'allegato 4 dell'avviso). L' interazione con l'utente potrà essere bidirezionale (richiesta di servizi, informazioni relative sull'avanzamento della propria pratica, etc)

8b. Benefici di GE.NE.SI. per gli operatori del sociale.

- una banca dati sulle associazioni stesse (fornita attraverso un apposito spazio su portale web)

- una banca dati di informazioni normative, pubblicazioni, convenzioni, atti, etc sul tema del Volontariato–Terzo Settore; (fornita attraverso un apposito spazio su portale web)
- sistema di incontro domanda / offerta tra Settore Pubblico e Volontariato-Terzo Settore; (fornita attraverso un apposito spazio su portale web)
- servizio di consulenza amministrativa e legislativa multicanale (Web e telefonica)
- creazione di una lista di discussione Web sul tema del volontariato
- realizzazione delle schede di presa in carico del cittadino/utente da parte del Volontariato-Terzo Settore (disponibili sia su Web che in forma cartacea)
- sistema di incontro domanda offerta tra settore privato e Volontariato Terzo settore

8c. Benefici di GE.NE.SI per la Pubblica Amministrazione.

- Formazione di una Base Informativa Statistica (Regione, ASL, Enti locali, associazioni Volontariato-Terzo Settore, questionari territoriali, INPS, Prefettura, ISTAT, ecc.) da cui nasce una modalità standardizzata di integrazione dei servizi del sistema sociale e sociosanitario dei soggetti contribuenti alla formazione della base informativa statistica
- Monitoraggio, controllo, programmazione, governo del sistema
- Revisione sostanziale delle modalità di scambio di dati tra Aziende Sanitarie, Comuni, Province, Terzo Settore e Regione Toscana
- accesso alle base dati integrata degli assistibili, delle strutture socio - sanitarie, delle strutture e dei servizi del volontariato-terzo settore e alle altre base dati integrate
- accesso, mediante il sistema di datawarehousing, alle informazioni in forma analitica o aggregata.

9. Il progetto e-R.ME.TE della Regione Toscana.

Dall'analisi delle esperienze fatte nel campo delle Tecnologie dell'Informazione e di alcune applicazioni specifiche nella sanità, risulta che la via della standardizzazione "estesa" di procedure e protocolli non è facilmente applicabile al complesso sistema sanitario.

L'uso di tecnologie del "Middleware"⁶⁴ anche su rete, l'individuazione delle unità minime di informazione in formato standardizzato per ciascun campo di applicazione, l'estensione d'uso di basi di dati su scala geografica, consentono di mantenere procedure e protocolli già sperimentati ed adatti alle singole attività.

Gli aspetti del "Middleware" cioè delle "Unità minime di informazione" viste come il prodotto di varie isole funzionali del sistema sanitario, assieme alla creazione di "Provider Medicali" costituiscono

⁶⁴ Insieme di interfacce che consentono la comunicazione tra gli applicativi locali, provvisti di specifico software, e l'archivio del sistema centrale.

l'architettura di base del modello di riferimento e rappresentano quindi una parte cruciale del progetto.

Definendo le unità "periferiche" come isole funzionali, esse sono integrate nel sistema clinico, accessibile per via telematica mediante la tecnica middleware salvaguardando gli investimenti e l'autonomia delle isole funzionali.

Per la consultazione remota e di primo accesso ai dati, si può sfruttare la metodologia WEB (HTML od Application-Server in Java), che consente la fruizione dei dati da parte di qualsiasi computer provvisto di browser, indipendentemente dal tipo, dalla piattaforma e dalla distanza.

Essendo presente nella maggior parte dei casi, un sistema di gestione amministrativa, consistente in una base di dati anagrafici del paziente, si può individuare una prima isola funzionale da integrare nel sistema centrale al fine di porre una prima pietra nella costituzione di un sistema che segua il paziente - cittadino nei suoi spostamenti attraverso l'immediata disponibilità dei suoi dati in caso di necessità.

Il concetto di "Provider Medicale" rappresenta l'evoluzione dell'architettura descritta: si tratta, infatti, di un servizio di hosting di dati e procedure relative applicazioni specifiche e ben collaudate di Telemedicina, accessibili attraverso la rete. I Provider Medicali offrono su connessioni "web based" i mezzi tecnici a livello di Server, hardware speciale, software e know-how, specifici per l'applicazione.

e-R.ME.TE è un progetto strategico di ricerca finalizzata predisposto dalla Regione Toscana nell'ambito dell'art. 12/bis D.lgs 229/99 del Ministero della Sanità.

Il progetto si propone di fornire al Servizio Sanitario Nazionale ed ai Servizi Sanitari delle Regioni e Province Autonome un sistema integrato, in grado di realizzare servizi continuativi, efficienti ed efficaci di Telemedicina. Il progetto prevede la definizione della metodologia, del modello gestionale, della sperimentazione e valutazione di prodotti e servizi di telemedicina per la classificazione, l'organizzazione, il rilascio e il loro trasferimento in aree geografiche determinate.

In particolare, il progetto mira a:

- Ridurre il carico quantitativo dell'assistenza, soprattutto infermieristica
- Ridurre l'accesso alle prestazioni istituzionalizzanti sviluppando forme anche avanzate, di home-care integrate con tutte le risorse specialistiche sanitarie e territoriali;
- Permettere una diffusione veloce delle informazioni specialistiche tra centri di ricerca e terapia, specialmente per quanto riguarda le immagini fisse o in sequenza di attività anatomo-metaboliche gestibili tramite appositi sistemi di interfacciamento guidato;
- Supportare i sistemi di emergenza/urgenza riducendo i tempi di accesso dei pazienti alle prestazioni e facilitando la pre-definizione di protocolli di intervento personalizzato;

- Ampliare le prestazioni del sistema sanitario e monitorarne l'efficacia sfruttando canali di collegamento già strutturati (reti, CUP, sistemi di controllo).

5. Problematiche connesse all'implementazione di un sistema di banche dati in ambiente socio-sanitario. Il fascicolo sanitario personale.

La cartella clinica è lo strumento utilizzato per la raccolta dei dati della storia clinica di un assistito, dati che vengono raccolti durante gli incontri con gli operatori sanitari, per la prevenzione o in occasione di episodi di malattia.

La diffusione dei calcolatori e delle reti telematiche sembra poter soddisfare le crescenti necessità di memorizzazione, elaborazione e trasmissione dei dati clinici, in un contesto più ampio di informatizzazione del sistema sanitario.

La gestione e il controllo della salute sono basati sull'uso, la trasmissione e il confronto di una grande quantità di dati, informazioni e conoscenze eterogenei.

Il bisogno di scambiare dati è aumentato vertiginosamente, sia all'interno di una struttura sanitaria (tra i diversi soggetti e tra unità operative specializzate), sia tra strutture anche geograficamente distanti.

L'innalzamento dei costi e la complessità dell'organizzazione richiedono un adeguato sistema informativo, che garantisca l'efficienza (attraverso l'ottimizzazione dell'organizzazione locale) e l'efficacia (attraverso la pianificazione e il controllo).

Viene quindi richiesto un trattamento uniforme di dati clinici e gestionali sui singoli e sulle strutture sanitarie, di letteratura scientifica e di protocolli, nell'ambito di sistemi informativi sempre più complessi ed estesi, spesso anche a livello internazionale.

Tradizionalmente, l'operatore sanitario lavorava in modo isolato, usando strumenti semplici ed economici per aiutare la propria memoria (per esempio, appunti su fogli bianchi o su schede prestampate in cartoncino).

La sanità attuale è invece caratterizzata da un insieme integrato di strutture, che cooperano al mantenimento o al ripristino del benessere del cittadino con molteplici operatori e funzioni, usando anche tecnologie sofisticate e costose. Ne risulta che i bisogni informativi e di comunicazione sono estremamente intensi e diversificati.

La cartella clinica "cartacea" nel frattempo è divenuta sempre più voluminosa, con documenti provenienti da moltissime fonti, e quindi risulta sempre più difficile trovare tempestivamente l'informazione necessaria.

In tutto il mondo si stanno ripensando, secondo un approccio informatico e telematico, sia i metodi usati finora per memorizzare e organizzare l'informazione clinica, che le procedure per scambiare e mettere in comune i dati tra operatori sanitari. Questo processo porterà in un prossimo futuro alla nuova cartella clinica elettronica (il "fascicolo sanitario personale"), pienamente inserita nell'era telematica.

11. Il Codice della privacy a proposito di protezione dei dati personali in ambiente sanitario.

Il confluire di dati personali in una banca dati, come la cartella clinica elettronica pone problematiche relative sia alla trattamento dei dati da parte di persone abilitate, sia un problema di conservazione di questi dati.

Il Codice della privacy, oltre agli obblighi del segreto professionale e d'ufficio, prevede l'adozione di una serie di misure di sicurezza di natura preventiva finalizzate a garantire una tutela oggettiva del dato trattato, prescindendo dalla natura del titolare o dal contesto in cui il trattamento si svolge.

Ne consegue, per l'ambito sanitario e socio-assistenziale, la necessità di applicare le diverse disposizioni settoriali già in vigore (HIV, procreazione assistita,), unitamente agli obblighi e alle misure di protezione indicate nell'art. 83 del Codice, oggetto di un provvedimento specifico emanato dal Garante nel novembre 2005.

Inoltre, occorre considerare le novità in tema di informativa e di acquisizione del consenso da parte dell'interessato, che può essere manifestato anche in forma orale purché documentato con annotazione dell'esercente la professione sanitaria o dall'organismo sanitario pubblico:

a) dignità dell'interessato (art. 83, comma 2, lett. e) del Codice

La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'interessato (artt. 2 e 83 del Codice).

b) riservatezza nei colloqui e nelle prestazioni sanitarie (art. 83, comma 2, lett. c) e d))

É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

c) notizie su prestazioni di pronto soccorso (art. 83, comma 2, lett. f))

L'organismo sanitario può dare notizia, anche per via telefonica, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica. La notizia o la conferma devono essere però fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso.

d) dislocazione dei pazienti nei reparti (art. 83, comma 2, lett. g))

Il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato.

e) distanza di cortesia (art. 83, comma 2, lett. b))

Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.

f) ordine di precedenza e di chiamata (art. 83, comma 2, lett. a))

All'interno dei locali di strutture sanitarie, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es., in caso di analisi cliniche), devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescindano dalla loro individuazione nominativa (ad es., attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione).

g) correlazione fra paziente e reparto o struttura (art. 83, comma 2, lett. h))

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato.

h) regole di condotta per gli incaricati (art. 83, comma 2, lett. i))

Il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate (artt. 30 e 29 del Codice).

12. Comunicazione di dati all'interessato.

Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico (individuato dallo stesso interessato, oppure dal titolare

del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es., un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare).

13. Altri adempimenti da rispettare.

I titolari del trattamento in ambito sanitario devono infine rispettare gli obblighi che attengono:

- a) alla notificazione al Garante;
- b) alla predisposizione dell'informativa da fornire agli interessati (art. 13 del Codice);
- c) all'acquisizione del consenso per i trattamenti di dati personali connessi all'erogazione delle prestazioni e dei servizi per svolgere attività di prevenzione, diagnosi, cura e riabilitazione (artt. 22, 26 e 76 del Codice);
- d) per gli organismi sanitari pubblici, al rispetto delle disposizioni contenute nel regolamento per il trattamento dei dati sensibili per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione adottato ai sensi dell'art. 20 del Codice;
- e) al rispetto delle autorizzazioni generali rilasciate dal Garante ed, in particolare, dell'autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (artt. 26 e 76 del Codice);
- f) alle misure di sicurezza (artt. 31-36 del Codice e allegato B) al Codice).

14. Il Documento Programmatico sulla Sicurezza (DPS).

A ciò devono aggiungersi le implicazioni e le problematiche connesse:

- all'implementazione di processi di e-government (finalizzati alla garanzia di efficienza ed efficacia nell'attività assistenziale);
- alla digitalizzazione dell'attività amministrativa, che comporta la necessità di costruire sistemi informativi a livello di ambito territoriale e a livello provinciale e regionale (Legge n. 328/00), allo scopo di organizzare il controllo e il monitoraggio della domanda e dell'offerta.

Una delle problematiche connesse alla costituzione di una banca dati sanitaria è appunto la sua conservazione.

Il Codice sulla Privacy prevede che entro il 31 marzo di ogni anno il titolare del trattamento dei dati personali e sensibili deve redigere il Documento Programmatico sulla Sicurezza (DPS). In tale documento devono essere indicate le misure minime adottate per assicurare un livello minimo di protezione dei dati, come previsto dal Disciplinare Tecnico allegato al Codice, contenente idonee informazioni riguardo:

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

- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto; la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto

dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Il documento deve essere conservato agli atti del professionista e non deve essere inviato ad alcuna Autorità.

L'Ufficio del Garante per la protezione dei dati personali ha ritenuto opportuno fornire alcune precisazioni relative ai trattamenti in ambito sanitario: nel rammentare che la notificazione deve essere effettuata solo se il trattamento è indicato dal Codice in materia di protezione dei dati personali e può essere esclusa per effetto di un provvedimento di esonero che è stato adottato dalla stessa Autorità, precisa tra l'altro sui seguenti argomenti:

14a. Dati genetici e biometrici

Sono esonerati dalla notificazione sia i professionisti che trattano dati genetici e biometrici individualmente, sia i medici che in forma associata condividono il trattamento con altri professionisti, specie all'interno di uno stesso studio medico. Il trattamento dei dati genetici non va notificato quando il professionista, nell'ambito di ordinari rapporti con il paziente, viene a volte a conoscenza di informazioni di tipo genetico (esame di screening o test genetici, indagini prenatali, diagnosi e cura di determinate patologie genetiche).

La notifica deve essere effettuata solo se il trattamento dei dati genetici è sistematico ed assume il carattere di costante e prevalente attività del medico (ad es. un genetista).

L'esonero non opera invece per i trattamenti di dati genetici e biometrici effettuati da strutture sanitarie pubbliche o private (ospedali, case di cura e di riposo aziende sanitarie laboratori di analisi cliniche, associazioni sportive). L'esonero è stato infatti disposto solo in favore di persone fisiche esercenti le professioni sanitarie e non per i trattamenti in quanto tali.

14b. Procreazione assistita, trapianti, indagini epidemiologiche, rilevazione di malattie mentali, infettive, diffuse e sieropositività

Le considerazioni sull'esonero espresse in tema di dati genetici e biometrici per i professionisti che effettuano il trattamento individualmente o in forma associata valgono anche per i trattamenti relativi a procreazione assistita, trapianti, indagini epidemiologiche, rilevazione di malattie mentali, infettive, diffuse e sieropositività.

Nell'esonero rientrano anche i trattamenti effettuati da un medico specialista nell'ambito di un'attività di consulenza o di procreazione assistita, sempre che non siano effettuati in modo sistematico. Per quanto riguarda malattie infettive il trattamento da notificare è solo quello che deve essere effettuato "a fini di ... rilevazione ..." di tali patologie e in linea generale riguarda gestori di strutture anziché singoli professionisti che occasionalmente vengono a conoscenza di tali.

14c. Prestazioni di servizi sanitari on line

Le prestazioni di servizi sanitari on line vanno notificate solo se i servizi sono:

- a) relativi ad una banca dati o siano prestati per via telematica
- b) relativi alla fornitura di beni.

Non vanno quindi notificati:

- a) i trattamenti di dati sanitari nell'ambito della teleassistenza (consultazione di specialisti per via telefonica)
- b) i trattamenti di dati organizzati in banche dati trattati manualmente (archivi cartacei)
- c) i trattamenti di dati organizzate in banche dati informatizzate ma non collegate ad una rete telematica Non devono, infine, notificare i medici che usano unicamente un computer nel proprio ufficio; usano la posta elettronica per dialogare con i pazienti, effettuano prenotazioni per gli assistiti, ecc.

Anche sulla base di altri esempi sono stati considerati quindi esonerati dalla notificazione diversi trattamenti effettuati nell'ambito della cd. medicina in rete. Per altri casi di accesso a banche dati da parte di medici è stato precisato che la notificazione compete invece alla ASL o all'ente locale.

15. Monitoraggio della spesa sanitaria; igiene e sicurezza del lavoro

Poiché non rientrano nel monitoraggio della spesa sanitaria non vanno notificati i trattamenti di dati sanitari effettuati da strutture convenzionate con il Servizio sanitario nazionale, solo per ottenere il rimborso delle prestazioni specialistiche erogate.

16. Valutazione economica di costi e benefici dell'integrazione di banche di dati in ambiente socio-sanitario.

Le grandezze economiche che figurano all'interno di piani, progetti, interventi, ecc., sono generalmente definibili in funzione dell'obiettivo che l'azione pubblica si propone. Criterio per la valutazione dell'agire dei soggetti pubblici è infatti quello secondo cui beni e servizi posseggono un valore che è determinato dall'impiego più redditizio tra quelli ai quali possono essere destinati: è il principio del costo – opportunità.

Il calcolo economico costituisce un insieme di regole utilizzabili per la valutazione degli effetti dell'agire pubblico sul benessere della collettività. Una delle forme più note del calcolo economico è l'analisi costi-benefici.

17. L'analisi costi-benefici.

è una tecnica usata per valutare la convenienza e se eseguire un investimento sul territorio in funzione degli obiettivi che si vogliono raggiungere.

L'analisi costi-benefici costituisce un complesso di regole (in senso lato) destinate a guidare le scelte pubbliche tra ipotesi alternative di intervento. Si distingue da altre forme di analisi destinate ad essere impiegate in decisioni economiche sia per gli obiettivi, sia per la scelta delle variabili. L'obiettivo consiste nel massimizzare i benefici sociali, o benessere collettivo, nell'area cui è responsabile la branca della Pubblica Amministrazione che compie l'analisi.

Le variabili sono rappresentate per lo più da beni che si presumono capaci di influire sugli obiettivi.

In alcuni casi, si tratta di beni di cui il mercato non fornisce valutazioni attendibili o condivisibili o non fornisce valutazioni del tutto.

La base su cui si fonda l'analisi è costituita dalle preferenze degli individui per i diversi assetti possibili che corrispondono alla realizzazione di ciascuna ipotesi alternativa.

Un'importante caratteristica dell'analisi costi – benefici: essa non fornisce valutazioni ricavate da una presunta “logica economica” distinta dalle altre (ad esempio dalla logica del politico e dell'amministratore), ma suggerisce criteri (desunti attraverso l'applicazione della razionalità economica convenzionale), per confrontare alternative di comportamento, il cui valore può essere determinato nei modi più vari e più soggettivi.

La scelta fra alternative progettuali costituisce una decisione in cui sono parti un “decisore” e la collettività.

18. Utilità.

Il concetto di utilità può essere assunto come equivalente a quello di preferenza. Nel concetto è implicita l'idea che gli effetti di una iniziativa (pubblica o privata), possano essere misurati sulla base dell'intensità con la quale sono percepiti.

Per individuare la possibile utilità della realizzazione di un progetto in ambito sanitario è logico operare con il metodo dell'indagine diretta in cui si definisce un campione di popolazione e si somministra un questionario adatto a rilevare soprattutto, la disponibilità a pagare a fronte della fruizioni di servizi socio-sanitari.

In particolare alle famiglie deve essere richiesto di precisare l'ammontare massimo di denaro che esse sarebbero state disponibili a pagare per un miglioramento del 50% della qualità dei servizi rispetto alla situazione attuale.

19. Il Metodo.

Proposto dall'analisi costi-benefici per effettuare le scelte fra le diverse alternative di intervento, classificato di regola come ordinalista,⁶⁵ consiste nell'accettare o respingere un progetto sulla base della possibilità di coloro che ricevono benefici dal progetto stesso, di compensare chi ne è danneggiato.

Un **progetto pubblico** costituisce una decisione di un soggetto della Pubblica Amministrazione che ha come scopo l'incremento del benessere della collettività compresa nella giurisdizione del soggetto decisore. L'elemento qualificante del progetto è il fatto di avere quale oggetto il benessere pubblico: la decisione di una ASL di acquistare o noleggiare una macchina o un impianto avrà effetti sui conti della ASL, ma non produrrà necessariamente conseguenze sul benessere della cittadinanza che vive nella giurisdizione della ASL.

Come ho detto prima, quando l'analisi dei progetti viene effettuata nella forma dell'analisi costi-benefici essi vengono espressi in termini monetari. I costi e i benefici che non possono per qualsiasi ragione essere monetizzati, non vengono inclusi nel calcolo.

L'esecuzione del progetto può avvenire da parte di due grandi categorie di soggetti economici: **l'operatore privato** e **l'operatore pubblico**.

L'**operatore privato** tende a porre a confronto i costi e i ricavi che derivano dalla realizzazione del progetto: si pone cioè in un'analisi, tipica delle scelte imprenditoriali, in cui l'obiettivo è costituito dalla *massimizzazione del profitto*.

Al contrario, **l'operatore pubblico** pone sul piatto della bilancia non solamente gli aspetti finanziari legati alle spese effettivamente sostenute per la realizzazione del progetto, ma individua una gamma di costi e di benefici che abbiano una relazione con l'obiettivo tipico delle scelte pubbliche: *massimizzazione del benessere sociale*.

Il risultato di progetti d'investimento privati può essere adeguatamente misurato attraverso il valore dei profitti o delle vendite (o attraverso il rapporto tra profitti o vendite e costi), dell'investimento stesso.

Opportuni confronti premetteranno di decidere quale tra le tante possibili alternative di un progetto privato risulta preferibile alle altre.

20. Differenze tra l'analisi finanziaria e l'analisi economica.

Ciò che rende diversa l'analisi finanziaria dall'analisi economica consiste nell'adozione da parte della seconda di una **prospettiva collettiva**.

L'adozione della prospettiva collettiva in luogo di quella privata porta ad escludere dal novero dei costi e dei benefici gli effetti che risultano essere meri trasferimenti di reddito interni alla collettività considerata.

Se **l'investimento è privato**, l'analisi costi-benefici assume i caratteri di un'analisi finanziaria: vengono cioè valutati i flussi monetari che nel corso

⁶⁵ La misura del benessere più frequentemente usata per i suoi evidenti vantaggi è rappresentata dal consumo, verificabili sul mercato attraverso l'osservazione del comportamento degli individui.

degli anni sono causati dall'investimento (positivi per quanto riguarda i ricavi; negativi per ciò che concerne i costi).

Se invece la valutazione riguarda un **investimento pubblico**, allora si è soliti parlare di analisi economica: ciò sta a significare che non si valutano solo i flussi finanziari, ma i costi e i benefici in senso lato, relativi a tutta la collettività.

In tale situazione si cerca di valutare in termini monetari tutti gli svantaggi (costi) e tutti i vantaggi (benefici) che l'investimento arreca alla popolazione interessata. Appare quindi come l'analisi della convenienza dal punto di vista pubblico prende in considerazione tutti quegli aspetti che possono influire sull'utilità degli individui interessati dal programma di investimento.

L'analisi economica risulta quindi più articolata e complessa dell'analisi finanziaria, infatti, mentre per quest'ultima i valori monetari presi in considerazione risultano essere di solito espliciti (per quanto riguarda i costi) o stimati (per quanto concerne i benefici), nell'analisi economica occorre ricorrere a giudizi di valore e a stime di larga massima per molti fattori che concorrono a formare i benefici ed i costi della collettività, caratterizzati spesso da elementi che sfuggono a qualsiasi criterio di misurazione (per esempio il miglioramento della qualità del paesaggio, la migliore salubrità dell'ambiente, ecc.).

21. Il ciclo del progetto

Il ciclo si distingue in quattro fasi: identificazione, preparazione, esecuzione e verifica dei risultati, che corrispondono ai momenti principali attraverso i quali l'idea di progetto passa prima di tradursi nel risultato desiderato.

22. Identificazione di costi e benefici.

Nel privato: i costi sono tutti i pagamenti effettuati per realizzare il progetto;

nel pubblico: beni e servizi ai quali si dovrà rinunciare per realizzare il progetto. La determinazione dei costi pertanto, implica il ricorso al concetto del costo-opportunità.

I benefici netti saranno rappresentati dai beni e servizi addizionali che vanno ad accrescere il benessere della collettività.

23. I criteri d'investimento

il rapporto costi-benefici tra 2 progetti: benefici (entrate) / costi (uscite).
Se il rapporto è > 1 , il progetto può essere accolto.

Fra numerosi progetti, sarà preferito quello che presenta il rapporto più elevato.

Questo criterio risulta particolarmente appropriato quando si tratta di stabilire un ordine di preferibilità tra diverse ipotesi progettuali in condizione di risorse limitate: esso ci consente infatti di incominciare a effettuare i progetti con il più alto valore di benefici per unità di capitale investito, raggiungendo via via, i limiti consentiti dalle risorse a nostra disposizione.

Il criterio Benefici / Costi può essere svitante in alcuni casi 1) se due progetti di dimensioni diverse si escludono l'un l'altro (si può porre rimedio sottraendo da quello più grande, benefici e costi, verificando che il rapporto sia positivo); 2) il rapporto Benefici / Costi può essere fuorviante a seconda di come si classificano i costi e i benefici: in generale un "beneficio" può essere considerato un risparmio di costi.

24. Problematiche di fondo nell'analisi costi-benefici

L'analisi costi-benefici si avvale delle metodologie monetarie, si devono tuttavia affrontare in pratica alcune importanti problematiche dovute principalmente al fatto che, dal punto di vista sociale, le spese e i ricavi previsti dal progetto in esame non rispecchiano gli effettivi costi e benefici. Infatti i prezzi reali che si utilizzano normalmente nelle analisi finanziarie rispecchiano il punto di vista di un singolo operatore, normalmente privato; occorre allora modificare i prezzi reali e trasformarli nei cosiddetti "prezzi ombra" che rappresentano i prezzi in grado di rappresentare al meglio il punto di vista della collettività (di solito i prezzi sul mercato immobiliare).

Più in generale l'analisi costi-benefici risente delle seguenti problematiche:

In alcuni casi prevalgono costi o benefici intangibili, non qualificabili monetariamente, perché inerenti a beni privi di un mercato (il valore della salute umana, del paesaggio, ecc.);

La sottovalutazione di costi o benefici che si verificano a lungo termine;

La scarsa capacità di partecipazione della collettività, in quanto per la persona comune è in genere molto difficile esprimere in termini monetari il grado di benessere che riceve da un bene ambientale, non disponendo al riguardo di validi e razionali parametri.

25. Costi espliciti e costi impliciti

Con questi termini si intendono rispettivamente i costi effettivamente sostenuti con un esborso monetario e quelli che, pur non essendo determinati da un pagamento effettuato, sono individuabili come costi in quanto hanno comportato *l'utilizzo di risorse interne all'azienda*.

Per esempio il noleggio di una macchina costituisce un costo esplicito, mentre l'uso di macchine aziendali è un costo implicito, perché non corrisposto realmente ogni volta che se ne fa uso, ma è rilevabile con

un'analisi economica basata su numerosi fattori (costo acquisto, durata economica, impiego annuo, ecc.).

26. Costi – opportunità

Nell'Analisi Costi - Benefici il concetto di costo deve essere considerato in un'ottica diversa da quella tradizionale (spese da sostenere per produrre un bene), che consideri adeguatamente le rinunce sopportate in relazione ai possibili impieghi alternativi del capitale investito.

Il costo così determinato, detto **costo-opportunità**, è pari al valore di mercato o di costo dei beni a cui si è dovuto rinunciare per poter disporre delle risorse necessarie ad acquistare il bene in esame.

27. Criteri secondo i quali deve essere determinato in saggio di sconto nell'analisi costi - benefici.

Un problema specifico dell'analisi costi-benefici è quello dello sconto. Infatti, l'Analisi Costi - Benefici valuta la convenienza a realizzare un investimento sulla base del confronto **benefici attualizzati** e i **costi attualizzati** derivanti dal progetto; ciò significa che occorre accumulare all'attualità tutti i benefici e i costi che si presentano in momenti diversi nel tempo.

Sorge quindi il problema dello **sconto** dei costi e dei benefici futuri, dato che questi non hanno il medesimo valore sociale dei costi e dei benefici presenti.

Sappiamo che le ragioni economiche di tale procedura risiedono nel fatto che a una somma di denaro che si materializza nel futuro è attribuito un valore inferiore di una somma, nominalmente identica, disponibile nel presente.

Si tenga comunque presente, che se consideriamo una società ricca, beni quali la salute, l'efficienza organica ecc., saranno valutati più di quanto non siano considerati in una società povera.

Teoricamente il tasso sociale di sconto dovrebbe rappresentare il tasso medio di tutti gli investimenti nei quali si potrebbe impiegare il denaro dei contribuenti, che viene invece prelevato dal sistema fiscale; del resto, le opere pubbliche possono essere considerate una forma forzata d'investimento dei capitali della collettività, la cui volontà è, però, mediata dall'organismo decisionale. In sostanza, quindi, il tasso viene fissato tramite precise scelte politiche.

Spesso si evidenzia il fatto che si dovrebbero usare più tassi sociali di sconto in relazione al tipo di opera o al reddito di chi viene investito dagli effetti della stessa. Attualmente in Italia si adotta un unico tasso, il che semplifica notevolmente il confronto tra investimenti, anche se dà luogo ad inevitabili errori (che comunque non pregiudicano la validità delle stime), generalmente esso varia fra il 5 e l'8%, tendendo presente che l'adozione di un

basso tasso di sconto sociale tende a privilegiare i progetti d'investimento a lungo termine.

Il **saggio sociale di preferenza temporale** esprime le condizioni alle quali gli individui sono disposti a privarsi della disponibilità del denaro e di rinviarla nel futuro.

Queste condizioni, espresse in pratica da un saggio di interesse, se sono riferite ad un'intera società esprimono la disponibilità a investire in opere pubbliche per avere benefici in tempi futuri.

È facilmente intuibile che anche la determinazione del saggio costituisce una fase delicata e importante e non facile nel processo di valutazione.

Il problema del saggio di sconto non è di facile soluzione; si può considerare

1. un saggio derivato dai titoli di Stato;
2. un saggio pagato per mutui contratti dalla collettività;
3. oppure una particolare interpretazione è quella di usare un saggio elevato di sconto per scoraggiare gli investimenti pubblici in una situazione di scarsa disponibilità di capitale; cioè il saggio diventa strumento di selezione dei progetti, consentendo di ottenere un equilibrio tra risorse ed impieghi.

28. Criterio di giudizio su un investimento basato sul valore attuale netto (VAN).

Un primo tipo di decisione inerente all'accettazione o al rifiuto del progetto può essere presa sulla base del *valore attuale netto* (VAN), che consiste nell'accettare un progetto se la somma dei suoi benefici (B) attualizzati, al netto dei costi (C) pure attualizzati è maggiore di zero.

Il VAN rappresenta una somma di denaro.

Una volta noto il cash-flow del progetto e un saggio di sconto che chiameremo "di riferimento", il VAN risulta:

$$VAN (= P) = \sum_{i=1}^n [(B_i - C_i) / (1 + r)^i]$$

In altre parole, data una somma di euro 1000,00 pagabile a distanza di n anni da questo momento (= periodo 0), il VAN di tale somma è la quantità di denaro che è necessario investire oggi, al saggio composto che è stato assunto come saggio di riferimento per ottenere euro 1000,00 alla fine degli n anni.

29. Criterio di giudizio su un investimento basato sul saggio di rendimento interno (SRI).

Un altro criterio che viene spesso suggerito è quello che tiene conto del cosiddetto *Saggio di Rendimento Interno* (SRI), questo consiste nel calcolare il tasso di sconto⁶⁶ che eguaglia il valore dei costi e dei benefici attualizzati. In pratica il SRI è quel saggio per cui si abbia un VAN uguale a zero.

Il SRI può essere ricavato solo per tentativi e, una volta trovato, può essere confrontato con un tasso di sconto predeterminato: se il primo è maggiore del secondo il progetto viene accantonato.

Formalmente il SRI è il saggio di sconto r per il quale risulta soddisfatta l'equazione:

$$\sum_{i=1}^n [(B_i - C_i) / (1 + r)^i] = 0$$

Il SRI può essere descritto tra l'altro, come il saggio di crescita medio di un investimento per unità di tempo.

criterio	svantaggi	Situazioni ideali
B-C	Viene massimizzato il rendimento del progetto in assoluto (non in relazione ai costi)	- Risorse illimitate - Progetti indipendenti
B/C	È sensibile alla definizione di B e C	- risorse limitate - progetti indipendenti
B/C applicato al progetto incrementale	È sensibile alla definizione di B e C	- risorse limitate - progetti dipendenti

Confronto fra VAN e SRI

	VAN	SRI
Caratteristiche	Numero assoluto	Saggio medio annuo
Controindicazioni	Non riflette il rischio di progetti "grandi"	- possibili valori multipli - dipende dalla durata del progetto
Campo d'applicazione ideale	- presenza di un saggio di riferimento - progetti non rischiosi	Assenza di un saggio di riferimento

30. L'analisi costi-efficacia.

⁶⁶ In matematica finanziaria lo "sconto" è la somma che si detrae da un capitale quando lo si vuole anticipare nel tempo; scontare o anticipare un capitale ha lo stesso significato.

Lo sconto (S_c) può essere conteggiato in due diversi modi:

- Sconto matematico o razionale;
- Sconto bancario o commerciale.

Può essere utilizzata quando i risultati di un intervento non sono omogenei; così si rende necessario prospettare una qualche forma di aggregazione delle diverse componenti che necessariamente è monetaria.

Questa analisi semplifica notevolmente il lavoro del valutatore in quanto consente di sostituire alle misure comprensive dei benefici e dei costi espressioni semplificate in termini monetari.

Spesso viene quantificato il valore dei progetti che comportano l'introduzione di innovazioni terapeutiche o organizzative in termini di costi risparmiati per unità di risultato prodotto. I risultati in questo caso è rappresentato da numero di vite salvate dal numero di mm cubi di pressione arteriosa eliminati, e simili. Ad esempio ci si può domandare qual è l'alternativa terapeutica che permette di salvare il maggior numero di vite a parità di costi, oppure qual è l'alternativa che permette di risparmiare la più alta somma di denaro per ottenere un dato numero di vite salvate.

L'analisi costi-benefici non trova larga applicazione in sanità proprio per la difficoltà nel valutare in termini monetari tutti i benefici ed i costi connessi con la realizzazione di un programma sanitario.

Infatti, l'analisi costi-benefici si è spesso arenata contro lo scoglio della difficoltà a fornire una valutazione monetaria di benefici intangibili dei programmi pubblici che influiscono sul rischio fisico.

Infatti, i giudizi di valore dei singoli individui differiranno a tal punto da rendere prive di senso le procedure di aggregazione necessarie per arrivare a valori globali degli interventi stessi.

Il decisore politico è quindi chiamato ad effettuare preliminarmente delle scelte delicate di ponderazione delle manifestazioni di volontà dei singoli individui.

31. Rischio ed incertezza

Fin qui abbiamo ragionato nell'ipotesi di conoscere i valori dei flussi di cassa degli investimenti. Talvolta si possono verificare delle variazioni o condizioni di incertezza, soprattutto se il progetto è a lunga scadenza.

Si rende quindi necessario operare delle scelte tra i possibili rischi in condizioni di incertezza.

Esistono alcune tecniche usate in condizioni di rischio:

- 1) ignorare il rischio. Si ci basa sulla convinzione che il rischio di uno solo fra i tanti già considerati sia pressoché ininfluenza per il rischio globale;
- 2) premio di rischio. Si procede ad una maggiorazione del tasso di sconto cosicché per accettare un investimento di si aspetta rendimenti più alti.
- 3) Moderazione delle valutazioni. Si diminuisce il valore atteso dei benefici e si aumenta quello dei costi a seconda del livello di rischio stimato.
- 4) Si procede all'effettuazione di misure statistiche.

Ma data la difficoltà a lavorare in condizioni di rischio, si preferisce agire in condizioni di incertezza, cioè con probabilità sconosciute.

Per agire in queste condizioni il primo passo è quello della costruzione di una *matrice dei benefici netti*.

Se per esempio, dobbiamo decidere fra 4 investimenti (A,B,C,D) in presenza di 3 possibili *eventi*, ad esempio tre diversi livelli della domanda nei confronti di 4 prodotti che possono verificarsi con probabilità ignote, avremo una tabella di questo tipo (i valori sono i benefici attesi):

eventi investimenti	1	2	3
A	25.000	45.000	40.000
B	125.000	100.000	-10.000
C	135.000	10.000	-20.000
D	10.000	150.000	50.000

Tabella dei benefici netti.

La regola del Maxmin. Minimax

Con la regola del maxmin sceglieremo quell'investimento che presenta il massimo tra i minimi benefici. E' un criterio che si usa se si vuole essere prudenti, e quindi è preferito in quelle situazioni nelle quali le condizioni finanziari non consentono di rischiare forti perdite. Per applicare il maxmin si rileva, per ogni riga della tabella, il valore minimo, e poi si sceglie l'alternativa che presenta il massimo tra questi valori minimi.

Nel caso proposto si ha:

A	25.000	←
B	-10.000	
C	-20.000	
D	10.000	

Sceglieremo quindi l'investimento A, che ci garantisce un beneficio minimo maggiore degli altri, ed un massimo beneficio di 45.000 unità monetarie se si verifica l'evento 2. Notiamo però che se si verificassero le condizioni corrispondente all'evento 2, l'investimento D ci darebbe un beneficio pari a 150.000 unità monetarie, per cui scegliendo A abbiamo perso l'opportunità di guadagnare $150.000 - 45.000 = 105.000$ unità.

Per minimizzare la massima perdita di opportunità si utilizza il seguente criterio del minimax.

Partendo dalla matrice dei benefici netti si costruisce una nuova tabella, detta tabella delle perdite condizionate di opportunità, scegliendo in ogni colonna dei della matrice dei benefici netti il valore più alto, e sostituendo ad ogni numero della matrice la differenza tra il massimo valore della colonna di appartenenza ed il numero stesso. Nel nostro caso il valore più alto nella prima

colonna è il 135.000, per cui sostituiremo il primo valore, pari a 25.000, con la differenza $135.000 - 25.000 = 110.000$, che ci dice che se scegliamo l'alternativa A, se si verifica l'evento 1 guadagneremo 25.000 unità, ma perdiamo l'opportunità di un ulteriore guadagno pari a 110.000 unità. Procedendo in questo modo avremo la seguente tabella:

eventi \ investimenti	1	2	3
A	110.000	105.000	10.000
B	10.000	50.000	60.000
C	0	140.000	70.000
D	125.000	0	0

Tabella delle perdite condizionate di opportunità.

A questo punto sceglieremo per ogni riga il valore massimo, cioè troveremo il pentimento massimo per ogni alternativa, e sceglieremo quella che presenta il minimo tra tali pentimenti massimi:

A	110.000	←
B	60.000	
C	140.000	
D	125.000	

L'alternativa da scegliere è quindi la B. L'uso di questo criterio comporta ovviamente una certa propensione al rischio, ma c'è il pericolo di perdere un buon guadagno per diminuire una perdita potenziale.

Per concludere, la scelta fra i due criteri dipende, oltre che dalla posizione psicologica del decisore circa il rischio, anche dai dati del problema, che possono da soli far cadere la scelta tra uno o l'altro criterio.

32. Classificazione dei costi.

I costi di realizzazione di un'opera della Pubblica Amministrazione, nell'analisi costi-benefici, vengono solitamente distinti:

- di tipo diretto: 1) costo di investimento che la P.A. deve affrontare per la realizzazione dell'opera; 2) costo di gestione, spese che l'Ente Gestore deve affrontare per rendere fruibile l'opera.
- di tipo indiretto: 1) costi di investimento per la realizzazione di opere complementari e necessarie per la fruizione dell'opera madre;
- mancati redditi nel dato contesto territoriale per effetto della presenza dell'opera;
- costi di esercizio per le nuove attività indotte dalla presenza dell'opera.

33. Classificazione dei benefici.

I benefici come i costi, vengono distinti in.

- di tipo diretto: 1) benefici che riguardano principalmente la P.A. che ha realizzato l'opera.
- di tipo indiretto: 1) benefici a vantaggio di opere complementari per effetto diretto dell'opera madre; 2) incremento di valore attribuito alla funzione della P.A. sul territorio di riferimento.

34. I tempi di attuazione dei costi e dei benefici.

La valutazione dei costi e dei benefici dovrebbe essere calcolata entro un arco di tempo di difficile determinazione:

- i costi di investimento, rispetto ai benefici, in linea di massima vengono sostenuti in momenti determinati dai tempi progettuali necessari per la realizzazione dell'opera;
- i benefici invece cominciano ad aversi gradualmente nel tempo durante e dopo la realizzazione dell'opera.

Convenzionalmente per la valutazione dei costi e dei benefici per le opere pubbliche viene considerata di circa 25 anni la durata economica dell'opera; per durata (o vita) economica si intende l'orizzonte temporale massimo oltre il quale i benefici netti attualizzati diventano insignificanti. Si definisce invece vita utile dell'opera il periodo oltre il quale essa non è più in grado di soddisfare la domanda per la quale è stata costruita.

35. Costi e benefici del progetto.

In relazione all'attività di presentazione di un progetto di miglioramento di servizi, individuo alcuni elementi da tener presenti:

1. descrizione tecnica;
2. localizzazione dell'intervento proposto;
3. caratteristiche tecniche e funzionali dell'intervento proposto.
Tecnologie adottate;
4. principali tipologie di intervento e indicazione dei parametri necessari per la valutazione;
5. subordinazione alla realizzazione del progetto alla realizzazione di altri interventi (costi, tempi e probabilità di realizzazione);
6. programmi e piani di lavoro del progetto proposto;
7. indicazione delle procedure da seguire per l'affidamento dei lavori relativi alla realizzazione del progetto;
8. calendario dei lavori;
9. aspetti istituzionali e organizzativi relativi alla realizzazione del progetto;
10. organizzazione, competenze, esperienze ed eventualmente struttura istituzionale del soggetto cui sarà affidata la realizzazione del progetto;
11. sistemi e metodo di verifica e controllo tecnico-amministrativo relativi alla realizzazione del progetto;

12. costi di realizzazione;
13. elencazione delle fasi di realizzazione distinguibili;
14. descrizione e quantificazione dei costi d'esercizio;
15. effetti sul sistema tariffario in vigore;
16. descrizione di rientri tariffari e non tariffari. Parametri adottati nella determinazione delle tariffe e standard di riferimento utilizzati (scaglioni tariffari, consumi specifici, qualità dei servizi);
17. piano finanziario;
18. vita economica dell'intervento proposto;
19. identificazione e quantificazione dei benefici economici diretti e indiretti, con indicazione dei metodi e procedure utilizzati;
20. descrizione di costi e benefici non quantificabili.

36. Costi e benefici dei programmi di prevenzione.

La letteratura riporta numerosi studi in cui i costi complessivi dell'intervento risultano inferiori ai costi evitati: questo è il caso dei programmi di prevenzione.

Esempio di applicazione

L'esempio di applicazione dell'Analisi costi-benefici in sanità si è sviluppato a partire da una pubblicazione (Demicheli, Jefferson, 1992) che analizza il rapporto costi-benefici dell'introduzione di un programma di prevenzione per l'epatite B.

L'analisi epidemiologica rivela un grado di endemicità intermedia per l'epatite virale acuta di tipo B in un Paese nel quale è in atto una strategia di prevenzione basata sulla vaccinazione dei gruppi ad alto rischio.

I risultati dell'analisi epidemiologica non sono ritenuti soddisfacenti e si vuole prendere in considerazione la possibilità di una vaccinazione di massa su tutti i nuovi nati.

Il Ministero della Salute, anche in considerazione dell'impegno economico richiesto da un programma del genere, decide di commissionare un'analisi costi-benefici per verificare la convenienza del programma.

L'epatite B

è una malattia virale endemica che ha manifestazioni acute e croniche, colpendo circa 300 milioni di persone in tutto il mondo. Ha dunque un notevole impatto dal punto di vista sanitario nei Paesi poveri e comporta un considerevole consumo di risorse nei Paesi ricchi.

Il virus dell'epatite B è coinvolto nella genesi della cirrosi e del carcinoma epatico; il vaccino antiepatite plasma-derivato scoperto negli anni Ottanta è risultato molto efficace nella prevenzione.

Ciò ha portato le autorità sanitarie di numerosi Paesi ad utilizzarlo per la vaccinazione di massa invece che per la vaccinazione dei soli gruppi ad alto rischio.

In questo esempio si analizza un caso in cui l'epatite si manifesta a un livello intermedio di endemicità con tasso di incidenza annuale pari a circa 6 casi per 100.000 abitanti, con ampia distribuzione geografica.

Un programma di vaccinazione mirata a gruppi con alto rischio ha raggiunto buoni livelli di copertura solo tra i lavoratori sanitari, con una scarsa adesione tra i gruppi a rischio.

Il Ministero della Salute, anche in considerazione di altri programmi di vaccinazione in atto (copertura 98% della popolazione a rischio) ritiene sia possibile ottenere ottimi risultati con un programma di vaccinazione di massa.

Tuttavia, prima di procedere decide di realizzare una valutazione costi-benefici mediante un modello economico basato su dati disponibili.

Prima di tutto bisogna valutare i benefici potenziali della vaccinazione. Come analisi di partenza si potrebbe intervistare un campione tratto dalla popolazione.

Tuttavia, trattandosi di una malattia alquanto complessa, si decide di procedere con una stima della frequenza annuale dei casi e delle risorse impiegate per ciascun caso tipico di epatite virale B. (I benefici vengono misurati come i costi evitati per la cura della malattia).

Viene rilevato il numero annuale dei casi suddivisi per età e sesso. I dati di costo sono rilevati grazie a studi di società scientifiche e dalle pubblicazioni in materia disponibili in letteratura.

Successivamente si cerca di definire il valore di un tipico caso di epatite B: grazie ai dati delle pubblicazioni in materia si costruisce un modello epidemiologico che riporta la storia dell'evoluzione della malattia sia nella fase cronica sia nella fase acuta.

Da tale modello si scopre che le fasi acute evolvono nell'arco di mesi, mentre quelle croniche nell'arco di molti anni.

In conclusione si dimostra come è sicuramente utile attivare un programma di vaccinazione ricavandone vantaggi economici per il risparmio sulle cure di casi cronici e per il numero di vite umane salvate.

37. Conclusioni.

Nel mondo occidentale siamo in presenza di un processo generale di riforma dei servizi di competenza statale, determinato dalla riduzione delle risorse complessive disponibili e, in ambito sanitario, dal progressivo invecchiamento della popolazione. In ambito sanitario, in particolare, coesistono oggi due grandi fenomeni dalle enormi implicazioni sui possibili modelli di politica sanitaria.

Innanzitutto è in corso una progressiva specializzazione tecnologica degli interventi clinici e, in seconda battuta, registriamo un aumento esponenziale del consumo di risorse finanziarie. In conseguenza di ciò, si sta

verificando un forte spostamento di bisogno/domanda di servizi verso le malattie croniche e cronicizzate, fattore che rende nodali i temi: “lungo degenza” e “continuità assistenziale”.

D'altra parte, ci si propone di mantenere la funzione di pubblica tutela della salute introducendo nuovi servizi finalizzati a migliorare l'efficienza complessiva del sistema.

In questo contesto, i Piani Socio Sanitari delle varie Regioni hanno evidenziato alcuni indirizzi ben precisi, ovvero cercare di rendere sempre più flessibile e disponibile la Pubblica Amministrazione verso il cittadino, punto di riferimento di tutta l'azione organizzativa, orientare la crescita dei servizi coniugando integrazione e competizione in una logica di rete, dare indicazioni per modelli operativo-gestionali che garantiscano compatibilità tra “bisogni” e “risorse” e, infine, controllare e regolare il sistema, attraverso la valutazione dei risultati prodotti dal sistema stesso, per confermare o modificare le soluzioni organizzative scelte.

In questa logica, i vari Sistemi Informativi Aziendali implementati attraverso i vari progetti realizzati, provvedono alla raccolta, all'elaborazione e alla restituzione di informazioni provenienti dai numerosi database creati in funzione delle attività socio-sanitarie.

Le informazioni, strutturate come report e analisi specifiche, devono supportare le azioni manageriali di programmazione, gestione e controllo previste dal piano organizzativo aziendale.

Per le Regioni è necessario quindi dotarsi di un sistema informatizzato che, attraverso avanzati criteri di acquisizione e interpretazione dei dati, effettui il “monitoraggio epidemiologico” nella sua forma più completa (analisi dei bisogni, rilevazione della domanda, controllo dell'erogazione delle prestazioni), permettendo di passare da un sistema diretto unicamente dall'offerta ad un sistema basato su comprensione dei bisogni e governo della domanda.

In generale, l'obiettivo dei vari progetti in corso di realizzazione è perseguire il superamento della fase di solo controllo a vantaggio di quelle di programmazione e di acquisto.

La strategia sottesa punta alla creazione di un sistema comprensivo di tutti gli attori (aziende sanitarie, erogatori privati, Medici di Medicina Generale/Pediatri di Libera Scelta, farmacisti, Organizzazioni Sindacali, enti locali, ecc.) che ruoti intorno alla figura dell'assistito. Sistema in cui l'ASL riveste una posizione centrale di verifica, stimolo, analisi, acquisto e controllo.

Gli aspetti principali del sistema riguardano il governo dell'offerta e il governo della domanda.

È chiara l'esigenza che il governo della domanda sia sempre più fondato sull'approfondimento di modelli e percorsi assistenziali, condivisi localmente con medici ed erogatori, volti a ricercare qualità del trattamento e miglioramento dell'efficienza.

Da qui il bisogno di basare valutazioni e risultati su un insieme di flussi informativi che consenta di cogliere gli elementi indispensabili al governo del sistema.

Vista la complessità dei fenomeni da “leggere” e la quantità dei dati in input, da un punto di vista tecnologico le tappe da considerare sono: l’implementazione di una banca dati e la predisposizione di un insieme di indicatori: di bisogno, domanda, offerta, performance e disponibilità di risorse.

Indicatori volti a superare il gap esistente tra gestione strategica e gestione corrente, e per monitorare nel breve/medio periodo il raggiungimento degli obiettivi strategici al fine di indirizzare il management verso la massimizzazione del rapporto risorse/benefici per gli assistiti.

Poiché, come si intuisce, questi sistemi di elaborazione delle informazioni poggiano sulla trasformazione del “dato” in “informazione”, il grado di utilità di quest’ultima dipende essenzialmente dall’esattezza dei dati disponibili, dalla rapidità di aggiornamento della situazione e dalla significatività degli indicatori in coerenza con gli scopi d’utilizzo.

In sintonia con questa strategia, il momento operativo riguarda l’attuazione di una completa integrazione tra le numerose banche dati (delle organizzazioni locali e statali e degli operatori privati), che hanno sempre avuto operatività e programmazioni separate e che quindi si sono rivelate poco utili alla vision globale.

C’è da rilevare che il settore sanitario italiano si trova generalmente impreparato di fronte al pervasivo uso delle nuove tecnologie dell’info-telematica, in quanto non dispone di una esperienza adeguata sui sistemi info-telematici a corollario del primario processo ospedaliero di assistenza.

Più precisamente questo processo primario è relativo alle attività clinico-ambulatoriali svolte sul paziente. Le informazioni raccolte dovrebbero confluire nella cartella clinica elettronica e nelle transazioni ad essa collegate (prescrizioni, referti, lettere di dimissioni, etc.).

Il sistema info-telematico e clinico-ambulatoriale di una struttura sanitaria richiederebbe l’integrazione sia con i sottosistemi amministrativi e epidemiologici e dell’alta direzione della struttura stessa, sia con i sistemi di gestione dell’informazione clinica di altre strutture sanitarie, nella logica della continuità assistenziale.

La maggior parte degli aspetti tecnologici non costituiscono al momento un ostacolo allo sviluppo. Le strategie, l’armonizzazione, i prodotti di qualità, le competenze sono invece insufficienti.

In conseguenza, le azioni necessarie per un armonico sviluppo dell’e-Sanità in Italia possono essere identificate come segue:

- completare le reti sanitarie regionali e le infrastrutture di base (hardware e software, formazione del personale)
- creare una info-struttura pubblica a livello nazionale
- promuovere l’introduzione delle transazioni elettroniche cliniche e gestionali
- favorire lo sviluppo della certificazione di qualità per l’e-sanità secondo gli standard internazionali (HL7, CEN, ISO)

- fornire servizi avanzati ai cittadini
- costruire indici nazionali dei cittadini, delle strutture sanitarie, dei servizi erogati, dei fornitori e dei prodotti (a partire dai registri regionali e dalle anagrafi informatizzate)
- costruire indici sulla documentazione clinica sul cittadino (cartella sanitaria individuale) e server per memorizzazione e accesso ai dati clinici dei pazienti
- favorire la raccolta e l'analisi di dati elementari per governance e supporto clinico, migliorare la raccolta dati e l'analisi relativa agli indicatori, sviluppando la capacità di analisi locale

Inoltre occorre creare un Osservatorio sull'e-Sanità, per:

- produrre materiale comparativo e linee guida all'implementazione (es. su strategie, soluzioni valide)
- fornire un supporto continuativo e documentato ai decisori pubblici locali
- sviluppare, attraverso un ampio dibattito nel Paese, una strategia, espandendo gli obiettivi "e-europe" in piani nazionali e regionali dettagliati
- promuovere la cultura e la diffusione degli standard di qualità

D'altra parte il Garante per la protezione dei dati personali è fatto destinatario di reclami e segnalazioni con quali si rappresenta una situazione dove alcune strutture sanitarie in Italia, nell'erogare prestazioni e servizi per finalità di prevenzione, diagnosi, cura e riabilitazione, non rispetterebbero le garanzie previste dalla legge a tutela, in particolare, della dignità e della riservatezza delle persone interessate.

Infatti, in materia di trattamento dei dati personali in ambito sanitario, il Codice prevede che gli organismi sanitari pubblici e privati adottino misure ed accorgimenti di carattere supplementare rispetto a quelle già previste per il trattamento dei dati sensibili e per il rispetto delle misure di sicurezza. In particolare, l'art. 83 individua alcune specifiche prescrizioni che devono tradursi anche in adeguate misure organizzative, ferma restando la necessità di adottare comunque tutti gli ulteriori accorgimenti che si rendessero opportuni per garantire il più ampio rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

La strada da percorrere nel settore dell'e-Sanità è lunga e difficile perché si deve riorganizzare tutto il sistema dell'assistenza, mettendo al centro delle attenzioni il paziente e per integrare le varie banche dati. Inoltre vi è un problema relativo alla formazione del personale sia tecnica, derivata dall'utilizzo delle tecnologie dell'ICT, sia giuridica per quanto riguarda la corretta trattazione dei dati personali dei pazienti stessi.

CAPITOLO IV

VINCENZO RUSSO

INTRODUZIONE AGLI ATTI AMMINISTRATIVI ELETTRONICI:
TRA DISCREZIONALITA' E VINCOLATIVITA'

SOMMARIO: 1. Considerazioni introduttive. – 2. Le diverse accezioni di atto amministrativo elettronico. – 3. I principali problemi del dell'atto amministrativo ad elaborazione elettronica. – 4. L'atto amministrativo elettronico discrezionale: appunti per una ricostruzione. – 5. l'atto amministrativo elettronico discrezionale e i sistemi esperti: uno sguardo al futuro.

1. Considerazioni introduttive

Anche nell'ambito dell'attività della pubblica amministrazione, così come per qualsiasi altro campo del diritto coinvolto dalla rivoluzione digitale, svolge un ruolo rilevante ai fini sistematici e classificatori la differenza tra *informatica giuridica documentale* e *informatica giuridica decisionale* (o *meta-documentale*).

Con la prima⁶⁷ si fa riferimento all'uso dei sistemi informatici al fine di permettere la raccolta e la sistemazione delle varie fonti giuridiche (intese qui in senso a-tecnico) esistenti, con particolare riguardo alle leggi e alle sentenze di un dato ordinamento giuridico, con lo scopo principale (ma non unico) di favorirne l'immediata reperibilità e il confronto istantaneo tra norme e decisioni.⁶⁸

Con il termine *informatica giuridica decisionale*, invece, s'intende l'impiego dei sistemi cognitivi elettronici al fine di applicare ed eseguire atti giuridici, siano essi leggi, sentenze o, per quanto interessa in questa trattazione, atti amministrativi, di modo che siano direttamente prodotti dal computer.⁶⁹ In tal caso, diversamente dall'*informatica documentale*, si passa direttamente a riprodurre in via automatica le varie attività del giurista, cioè a dare soluzioni "ai" problemi e non a dare una mera documentazione "sui" problemi.

⁶⁷ Cfr. A. E. PERÈZ LUÑO, *Saggi di Informatica Giuridica*, Milano, 1998, pp. 39 ss.; R. BORRUSO, C. TIBERI, *L'informatica per il giurista. Dal bit a internet*, 2ª ed., Milano, 2001, p. 653.

⁶⁸ Si tratta di una branca dell'informatica giuridica particolarmente sviluppata, in quanto ne costituisce storicamente il primo ramo d'applicazione. Si pensi, già prima dell'avvento di Internet, all'attività svolta dal Centro Elaborazione Dati della Corte di Cassazione. Sul punto cfr. per uno sguardo d'insieme R. BORRUSO, C. TIBERI, *L'informatica...*, cit., pp. 654 e 660 e più specificamente R. BORRUSO - L. MATTIOLI, *Computer e documentazione giuridica. Teoria e pratica della ricerca*, Milano, 1999. Per una sintesi delle principali banche dati italiane e internazionali cfr. M. RAGONA, *Banche dati e sistemi informativi giuridici*, in: R. NANNUCCI (a cura di), *Lineamenti di informatica giuridica. Teoria, metodi, applicazioni*, Napoli-Roma, 2002, pp. 247 ss.

⁶⁹ Cfr. A. MASUCCI, *L'Atto amministrativo informatico, Primi lineamenti di una ricostruzione*, Napoli, 1993, p. 13, "il computer, invero, può oggi definire esso stesso [...] il contenuto di un regolamento d'interessi; può produrre esso stesso atti amministrativi...".

Attraverso le istruzioni contenute nel programma informatico, infatti, si permette al computer di svolgere un ragionamento molto simile, nella sua struttura, a quello umano, che consiste nell'applicare una serie di passaggi logici ad una determinata premessa per giungere ad una specifica conclusione.⁷⁰ L'elaboratore, in sostanza e diversamente da altre macchine costruite dall'uomo, permette di condurre a risultati che non sono prevedibili a priori, nonostante tutte le operazioni che esso compie siano predefinite dal programmatore.⁷¹

Ciò non toglie che l'informatica decisionale si presenta strettamente e direttamente connessa all'informatica documentale, visto che (per usare le parole di Jean Frayssinet)⁷² il computer-funzionario ha bisogno del computer-archivio per potersi attivare con cognizione di causa: tutte le informazioni che gli occorrono devono essere messe a sua disposizione attraverso il previo inserimento nella memoria del computer.⁷³

2. Le diverse accezioni di atto amministrativo elettronico

Fatta questa doverosa premessa, per quanto qui interessa occorre distinguere tra atto amministrativo *in forma elettronica* e atto amministrativo *ad elaborazione elettronica*.⁷⁴

Nel primo caso ci si riferisce all'atto emanato mediante supporto informatico, per cui quest'ultimo è elettronico in quanto si fonda su materiale elettronico⁷⁵: è la forma che lo denomina, non il contenuto, che rimane determinato dal funzionario.

L'atto in forma elettronica ha cominciato ad essere preso in considerazione dal legislatore italiano solo a partire dai primi anni '90 del

⁷⁰ Si ricorda che i passaggi che permettono di giungere dall'*input* all'*output* costituiscono un *algoritmo*, inteso nel senso tecnico del termine come successione ordinata di operazioni predeterminate.

⁷¹ Cfr. R. BORRUSO, *La legge, il giudice, il computer. Un tema fondamentale dell'informatica giuridica*, Milano, 1997, pp. 22 e 23: "...il computer non è libero: fa solo quello che gli è stato comandato di fare. Tuttavia presenta spesso margini notevoli di imprevedibilità. Libertà e imprevedibilità non sono la stessa cosa...".

⁷² Citato da A. MASUCCI, *L'Atto amministrativo...*, cit., p. 13: "...è possibile andare oltre la gestione (per quanto sofisticata) dei dati e affidare al computer compiti finora riservati all'uomo: è possibile passare dalla fase del «computer-archivio» alla fase del «computer-funzionario»...".

⁷³ Sul punto approfonditamente A. NATALINI, *Sistemi informativi e procedimenti amministrativi*, in *Riv. trim. dir. pubbl.*, n. 2, 1999, pp. 449-471.

⁷⁴ Cfr. C. GIURDANELLA, E. GUARNACCIA, *Elementi di diritto amministrativo elettronico*, Macerata, 2005. Si veda anche D. BRUNETTI, *Il codice della amministrazione digitale e la gestione elettronica dei documenti*, in *Comuni d'Italia*, n. 10, 2005, pp. 21-24.

⁷⁵ La terminologia in esame è stata introdotta da G. DUNI, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, ora rinvenibile alla url www.privacy.it/duni19780601.html e *teleamministrazione*, voce dell'Enciclopedia Giuridica Treccani, vol. XXX, Roma, 1993, p. 381 ss.; cfr. anche A. MASUCCI, *L'atto amministrativo elettronico*, Napoli, 1993; B. SELLERI, *Gli atti amministrativi in forma elettronica*, in *Dir. soc.*, n. 1, 1982, p. 133; M. MINERVA, *L'attività amministrativa in forma elettronica*, in *Il foro amm.*, n. 4, 1997, p. 1300 ss.; A. USAI, *Le prospettive di automazione delle decisioni Amministrative in un sistema di teleamministrazione*, in *Dir. inf. inform.*, n. 1, 1993 pp. 164 ss.

secolo scorso, sulla spinta riformistica conseguente al varo della legge sul procedimento amministrativo.⁷⁶ Infatti, fino agli inizi del decennio scorso il diritto amministrativo si occupava ancora essenzialmente del solo documento amministrativo cartaceo, ossia di un documento incorporato su carta e caratterizzato dalla sua appartenenza alla P.A. (in quanto formato dal potere pubblico o in ogni caso da questo acquisito).⁷⁷

In realtà la dottrina giuridica era pressoché unanime nell'affermare che non necessariamente il supporto dovesse essere cartaceo, potendo benissimo consistere in qualunque materiale idoneo alla rappresentatività di un fatto o di un atto.⁷⁸ Per cui in realtà la scelta legislativa era nient'altro che un ossequio alla tradizione e alla prassi vigente.

L'evoluzione tecnologica fa emergere, infatti, nuovi supporti materiali sui quali riportare i documenti. Non a caso la legge 241/90 sul procedimento amministrativo, all'art. 22, c. 2, descrive già modernamente il documento amministrativo come “ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale”:⁷⁹ il richiamo alle rappresentazioni elettromagnetiche consentiva e consente, dunque, il riconoscimento nell'ordinamento positivo proprio di uno strumento fondamentale quale quello di *documento amministrativo elettronico* e, per converso, lasciava e lascia intendere l'esistenza e il riconoscimento nel nostro diritto dell'*atto amministrativo elettronico*.⁸⁰

⁷⁶ Per una breve storia del documento amministrativo elettronico può rinviarsi a L. STILO, *Il documento elettronico nella società dell'informazione*, in *Il Nuovo diritto*, n. 9, 2004.

⁷⁷ A. M. SANDULLI, voce *Documento (dir. amm.)*, in *Enc. dir.*, XIII, Milano, 1964, p. 607. In proposito non può non ricordarsi la legge 4 gennaio 1968 n. 15 (abrogata dall'articolo 77, comma 2, del d.P.R. 28 dicembre 2000, n. 445 ossia il T.U. sulla documentazione amministrativa) la quale imponeva ai documenti originali la redazione a stampa, con scrittura a mano o a macchina. Per un'analisi della legge citata cfr. U. EVANGELISTI, *Documentazione amministrativa: Legalizzazione e autenticazione di firme. Rilascio di copie di atti*, II ed., Firenze, 1971.

⁷⁸ F. CARNELUTTI, voce *Documento (teoria moderna)*, in *Novissimo Digesto Italiano*, VI, 1957, p. 86: “...ma il vero è che qualunque materia, atta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo...”. Cfr. anche M. S. GIANNINI, voce *Atto amministrativo*, in *Enc. dir.*, IV, Milano, 1959, p. 178 “...i provvedimenti amministrativi più importanti assumono questa forma di esternazione più per prassi che per statuizione di norma; ma se essa non viene osservata, e si ha altra forma di esternazione, più succinta e meno maestosa, non perciò vi è vizio del provvedimento...”

⁷⁹ Testo aggiornato in base all'art. 15 della legge 11 febbraio 2005, n. 15 che modifica e integra la legge 241/90. l'articolo originale definiva il documento amministrativo come “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”.

⁸⁰ Si parla anche di atto informatico, digitale o virtuale, così come il documento viene chiamato tanto informatico quanto elettronico. Ovviamente si parla di atto in quanto presupposto del documento: il documento amministrativo elettronico è il documento rappresentativo dell'atto amministrativo elettronico. Ecco perché, con i chiarimenti di cui abbiamo parlato nel testo, si può parlare indifferentemente di atto o documento amministrativo elettronico, a seconda del punto di vista

Quest'ultimo, come si è accennato, può anche essere definito con l'accezione di atto amministrativo ad elaborazione elettronica.⁸¹ In tal senso ci si riferisce ad una completa automazione dell'atto: qui è il contenuto ad essere elettronico e non necessariamente la forma,⁸² visto che è lo stesso computer, tramite un apposito programma informatico, a determinare l'atto amministrativo. L'attività umana in questo caso si limita soltanto alla realizzazione del *software* che permettere al calcolatore, una volta fornitegli tutte le informazioni necessarie, di predisporre l'atto o il provvedimento.

A tal proposito si può tracciare un parallelismo tra procedimento amministrativo e attività svolta dal computer.⁸³

E' noto che per procedimento amministrativo s'intende, genericamente, "una serie coordinata e collegata di atti e di fatti imputati ad organi e soggetti diversi tendenti nel loro insieme alla produzione di un effetto giuridico".⁸⁴ La legge 241/90 ha recepito gli insegnamenti dottrinali che normalmente scompongono il procedimento nelle quattro fasi dell'iniziativa (ad istanza di parte o d'ufficio), dell'istruttoria (acquisizione, gestione e valutazione di tutte le informazioni utili), della decisione (adozione del provvedimento finale) e dell'eventuale integrazione dell'efficacia (concernente i controlli e la pubblicazione del provvedimento).⁸⁵

Stando così le cose, si può stabilire una netta corrispondenza tra il provvedimento amministrativo e il "prodotto" (l'*output*) per il quale è predisposto il programma informatico: in entrambi i casi si tratterà dell'atto finale di un dato procedimento; stesso parallelismo, quanto meno parziale, si ha tra l'iniziativa e l'istruttoria nel procedimento amministrativo e l'inserimento e la raccolta dei dati nella macchina: in tal caso sarà il computer a valutare le condizioni di ammissibilità, i requisiti di legittimazione ed i presupposti che sono rilevanti per l'emanazione del provvedimento, come stabilito dall'art. 6 della legge 241/90.⁸⁶ Così, ad es., l'inserimento nel

adottato. D'altronde, la stessa legge 241/90 ha eliminato l'endiadi "atti e documenti" contenuta nella legislazione precedente per parlare esclusivamente di documento. Cfr. C. GIURDANELLA, *L'atto amministrativo elettronico*, in F. SARZANA DI SANT'IPPOLITO, *E-government*, Piacenza, 2003, p. 33 ss.

⁸¹ Sul punto, oltre alla bibliografia richiamata alle note precedenti: V. BUSCEMA, *Discrezionalità amministrativa e reti neurali artificiali*, in *Il foro it.*, n.2-3, 1993, p. 620; A. SCALA, *L'automazione nella redazione degli atti amministrativi*, in *Nuova rass.*, n. 4, 1995, pp. 1792 ss.

⁸² Infatti il concetto di atto ad elaborazione elettronica è distinto dalla questione della forma elettronica, nel senso che è possibile che l'atto predisposto dall'elaboratore debba essere stampato e firmato dal funzionario responsabile per acquistare validità, inerendo così alla tradizionale forma cartacea. E' ovvio però che in una società completamente teleamministrata l'atto elaborato dal calcolatore acquista la validità direttamente nella versione informatica, così che l'elaborazione elettronica e la forma informatica del provvedimento vanno di pari passo. Cfr. G. DUNI, *Teleamministrazione...*, cit., p. 5 ss.

⁸³ Sul punto M. G. LOSANO, *L'informatica e l'analisi delle procedure giuridiche*, Milano, 1989, in cui si prendono in esame sia l'analisi del procedimento legislativo che quella del procedimento amministrativo sulla base di diagrammi di flusso informatici.

⁸⁴ Com'è comprensibile, la letteratura sul procedimento amministrativo è molto vasta. Ci limitiamo, pertanto, a rinviare a E. CASETTA, *Manuale di diritto amministrativo*, Milano, 2005. F. CARINGELLA, L. DELPINO, F. DEL GIUDICE, *Diritto Amministrativo*, Napoli, 2004.

⁸⁵ Ancora E. CASETTA, *Manuale...*, cit., pp. 212-218.

⁸⁶ Questo il tenore letterale dell'art. 6 della legge sul procedimento amministrativo: "Il responsabile del procedimento:

calcolatore delle caratteristiche dell'immobile potrà portare ad emanare infine un atto computerizzato (cioè un provvedimento) di concessione edilizia. Sotto il profilo dell'articolazione del procedimento amministrativo non sembra sussistere, insomma, nessun tipo di ostacolo all'automazione.⁸⁷

3. Le principali problematiche sull'atto amministrativo ad elaborazione elettronica.

E' indubbio, per quanto fin qui osservato, che tra le varie funzioni a cui può essere adibito il calcolatore nell'ambito della P.A., quelle relative alla produzione automatica di atti amministrativi sono decisamente le più complesse e affascinanti; in tali casi, infatti, l'elaboratore non svolge più solamente un ruolo ausiliario all'attività decisionale dei funzionari, ma si sostituisce all'uomo stesso nel momento della determinazione del contenuto del provvedimento, divenendo a tutti gli effetti, come si diceva *supra*, un vero e proprio funzionario pubblico.⁸⁸

Il fatto che al calcolatore sia rimessa la decisione sul contenuto di un atto amministrativo significa, in termini informatici, che esso è stato *programmato* per predisporre il provvedimento, cioè che è stato istruito affinché possa svolgere determinate operazioni. E' palese che se qualora sia il calcolatore a predisporre atti amministrativi sulla base di quella serie di istruzioni che costituiscono il programma informatico, l'attività umana che è alla base della predisposizione e del contenuto dell'atto si sposta ancora più a monte: invece di dedicarsi all'emissione dei singoli provvedimenti, il funzionario "umano" passa alla realizzazione del programma che, appunto, permetterà al computer di approntare, volta per volta, gli atti necessari.⁸⁹ Resta inteso, su tale base, che il *software*, ossia l'insieme delle istruzioni date al

a) valuta, ai fini istruttori, le condizioni di ammissibilità, i requisiti di legittimazione ed i presupposti che siano rilevanti per l'emanazione di provvedimento;

b) accerta di ufficio i fatti, disponendo il compimento degli atti all'uopo necessari, e adotta ogni misura per l'adeguato e sollecito svolgimento dell'istruttoria. In particolare, può chiedere il rilascio di dichiarazioni e la rettifica di dichiarazioni o istanze erranee o incomplete e può esperire accertamenti tecnici ed ispezioni ed ordinare esibizioni documentali;

c) propone l'indizione o, avendone la competenza, indice le conferenze di servizi di cui all'articolo 14;

d) cura le comunicazioni, le pubblicazioni e le modificazioni previste dalle leggi e dai regolamenti;

e) adotta, ove ne abbia la competenza, il provvedimento finale, ovvero trasmette gli atti all'organo competente per l'adozione". L'art. 4, della legge 15/2005 di riforma della legge 241/90 aggiunge alla lett. e) della disposizione qui riportata anche il seguente periodo: "L'organo competente per l'adozione del provvedimento finale, ove diverso dal responsabile del procedimento, non può discostarsi dalle risultanze dell'istruttoria condotta dal responsabile del procedimento se non indicandone la motivazione nel provvedimento finale".

⁸⁷ Cfr. A. MASUCCI, *L'atto...*, cit., p. 48.

⁸⁸ Il primo ad esprimersi in questo modo è V. FROSINI, *L'informatica e la pubblica amministrazione*, in *Riv. trim. dir. pubb.*, n. 2, 1983, p. 484.

⁸⁹ "I programmi informatici [...] non sono che sequenze di ordini o precetti che la macchina elettronica deve eseguire in circostanze predeterminate, cosicché anche di essi è certamente possibile il controllo giurisdizionale": così la sentenza rivoluzionaria del Consiglio di Stato, sez. VI del 7 febbraio 1995, n. 152, in *Foro amm.*, n. 1, 1995, p. 364, in cui si afferma che l'azione amministrativa che si avvale dell'uso di procedure informatizzate e di macchine elettroniche non si differenzia in alcun modo da quella amministrativa ordinaria.

calcolatore affinché questi realizzi determinate funzioni e attività, non coincide di per sé con l'atto amministrativo, ma ne costituisce solo il prodromo, e dunque consta esclusivamente in uno strumento di ausilio all'autorità amministrativa.⁹⁰

Tutto ciò c'introduce al primo dei problemi da affrontare quando si è alla presenza di un atto automatizzato, ossia al problema concernente quell'elemento essenziale dell'atto amministrativo quale la volontà, l'assenza della quale determina giuridicamente l'inesistenza dell'atto stesso.⁹¹

Ci si chiede, insomma, se l'atto amministrativo emanato da un elaboratore sulla base di un dato programma possa integrare l'elemento volontario, pena la conseguente invalidità dello stesso.⁹² La dottrina amministrativistica più attenta ha rilevato, però, che nel caso di atti e provvedimenti amministrativi la volontà è definibile come volontà procedimentale:⁹³ la sola volontà che rileva è la volontà dell'atto e non del contenuto dell'atto, il quale non è interamente determinato dall'autorità emanante.⁹⁴

Insomma, la volontà procedimentale è il risultato della concertazione tra più uffici ed organi, ognuno dei quali ha una parte nell'assunzione della decisione finale e in cui non rileva affatto il momento psichico dell'organo a cui è imputabile il provvedimento finale.⁹⁵ Se questo è vero, allora l'atto amministrativo ad elaborazione elettronica non difetta affatto di volontà perché, nonostante il suo contenuto non sia stato puntualmente individuato dall'organo emanante, questo è pur sempre voluto dall'autorità procedente, la quale decide di affidare al computer tale compito e predispone le stesse

⁹⁰ Si può dire che "il software è uno strumento dell'agire amministrativo e nulla più": A. G. OROFINO, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Foro amm.*, n. 9, pp. 2273-2277 ed ivi bibliografia citata. Basti pensare, come ulteriore giustificazione di tale assunto, che se si trattasse di un vero atto amministrativo (*rectius*: documento) dovrebbe essere sottoscritto (con firma digitale); ma se si pone a mente che il programma informatico si compone di una pluralità di *file* (tutti passibili di propria sottoscrizione), alcuni dei quali soggetti a modifiche continue che ne impediscono l'immodificabilità, non appare logico apporvi proficuamente una firma digitale o, meglio, l'eventuale sua apposizione non avrebbe alcuna utilità. Sul punto cfr. P. RIDOLFI, *Firma elettronica: tecniche, norme, applicazioni*, Milano, 2003, *passim*.

⁹¹ Oltre a rinviare alla manualistica citata alla nota 18, si veda anche V. R. PERRINO, *L'atto amministrativo informatico e le cause della sua invalidità*, presso la url: www.amministrazioneincammino.luiss.it/site/.

⁹² Cfr. da ultimo R. CLARIZIA, *Il documento informatico sottoscritto: alcune note a margine del codice dell'amministrazione digitale*, in *Diritto dell'Internet*, n.3, 2005, pp. 221-225.

⁹³ Si veda M. S. GIANNINI, voce *Atto amministrativo*, in *Enc. Dir.*, IV, 1959, pp. 174 ss. il quale afferma che "...la volontà del provvedimento amministrativo, non è una volontà psicologica, né personale: il provvedimento passa per più uffici, e quindi è frutto del concorso di un numero piuttosto elevato di persone fisiche. Storicamente, in esso la volontà si presenta come un'astrazione e, giuridicamente, come un'ipostasi...". Nello stesso senso B. G. MATTARELLA, *Il provvedimento*, in S. CASSESE, *Trattato di diritto amministrativo*, Milano, 2005, pp. 744 ss.

²⁷ Cfr. A. G. OROFINO, *L'automazione amministrativa: imputazione e responsabilità*, in *Giornale di diritto amministrativo*, n.12, 2005, pp. 1300-1312.

²⁸ Così A. G. OROFINO, *La patologia...*, cit., p. 2257

istruzioni di cui si compone il programma su cui si basa l'attività dell'elaboratore.⁹⁶

Ma ciò che ci si chiede, ed è il secondo e definitivo problema da affrontare in questa sede, è se sia possibile o meno predisporre atti discrezionali della P.A. in modo del tutto automatico, da parte del computer.⁹⁷ Secondo la ricostruzione classica,⁹⁸ l'emanazione di un atto amministrativo è considerata discrezionale quando la legge permette all'amministrazione di operare una scelta in ordine ad un dato provvedimento, scegliendo tra più soluzioni tutte ugualmente legittime.⁹⁹ La scelta fra le diverse possibilità deve essere imperniata su una ponderazione degli interessi, pubblici e privati, coinvolti nel procedimento, che permetta di far prevalere l'interesse pubblico di primaria importanza con il minor sacrificio possibile degli altri interessi meritevoli di protezione.

La discrezionalità verte fondamentalmente su quattro caratteri del provvedimento, che sono l'*an* (la valutazione se emettere o no un determinato atto), il *quid* (la determinazione del contenuto dell'atto), il *quomodo* (la scelta della forma del provvedimento) e il *quando* (la decisione del momento in cui emetterlo). La scelta dell'amministrazione nell'emettere un atto discrezionale deve sempre essere operata entro i limiti dell'interesse pubblico (che deve prevalere comunque sugli interessi privati), della causa del potere (ossia delle finalità per le quali la legge ha attribuito il potere) e dei precetti di logica e imparzialità (per cui non potrà essere emesso un atto dal contenuto contraddittorio o irragionevole).

Com'è noto, nel caso in cui la discrezionalità oltrepassi queste soglie, il vizio che viene a configurarsi è l'eccesso di potere.¹⁰⁰ Tale vizio di legittimità dell'atto amministrativo, va qui detto per mera completezza, si verifica anche

⁹⁶ Cfr. A. MASUCCI, *L'atto...*, cit., pp. 85 ss.

⁹⁷ Sul punto D. DE PRETIS, *Valutazione amministrativa e discrezionalità tecnica*, Padova, 1995, pp. 27 ss e M. NATOLI, *Ambiti di operatività della discrezionalità amministrativa e di quella tecnica alla luce dell'informatizzazione dell'attività amministrativa*, in *Rass. avvoc. dello stato*, n. 2, 2004, pp. 712-730.

⁹⁸ Sulla discrezionalità amministrativa si rinvia alla manualistica citata. Inoltre cfr. S. PIRAINO, *La funzione amministrativa fra discrezionalità e arbitrio*, Milano, 1990 e A. PIRAS, voce *Discrezionalità amministrativa*, in *Enc. dir.*, XIII, Milano, 1964.

⁹⁹ Cfr. A. MASUCCI, *L'atto...*, p. 31. È tuttavia da ricordare l'esistenza di posizioni minoritarie in dottrina: teorie volte a dimostrare da una parte l'inesistenza del vincolo totale (perché ogni norma conterrebbe un margine di elasticità nel dettare un comportamento), e, dall'altro versante, l'impossibilità di una reale discrezionalità (perché ogni norma deve dare origine, comunque, a quell'unico comportamento dell'amministrazione che soddisfi meglio di ogni altro l'interesse pubblico). A questo proposito, cfr. U. FANTIGROSSI, *Automazione e Pubblica Amministrazione*, Bologna, 1993, pp. 71 ss.

¹⁰⁰ Sull'eccesso di potere come cattivo uso della discrezionalità amministrativa si veda la sentenza del C.d.S., sez. IV, del 16 ottobre 1995, n. 821, in *Foro amm.*, n. 5, 1995, p. 2164 e, più recentemente, la sentenza del C.d.S., sez. V, del 22 febbraio 2001, n. 984, in *Foro amm.*, n. 2, 2001, p. 452. In dottrina cfr. P. GASPARRI, *Eccesso di potere (dir. amm.)*, in *Enc. dir.*, XIV, Milano, 1965, pp. 126 ss.; F. MODUGNO – M. MANETTI, *Eccesso di potere. Eccesso di potere amministrativo*, in *Enc. giur.*, X, Roma, 1989; G. SALA, *L'eccesso di potere amministrativo dopo la legge 241/1990: un'ipotesi di ridefinizione*, in *Riv. trim. dir. amm.*, n. 2, 1993, pp. 175 ss.

in caso di difetto di motivazione ex art. 3 della legge 241/90,¹⁰¹ poiché la difficoltà di comprensione del linguaggio macchina e l'impossibilità di comprendere quali siano i passaggi che hanno portato all'emanazione dell'atto, priverebbero il cittadino della facoltà di capire bene le ragioni della decisione amministrativa e quindi, in buona sostanza, del diritto di far valere eventuali illegittimità della stessa.¹⁰²

Entro i limiti così posti, invece, la scelta discrezionale è da considerarsi insindacabile.¹⁰³ Quindi l'attività amministrativa sarà discrezionale se si ha almeno un elemento (*an, quid, quomodo* o *quando*) che non sia fissato dalla legge; viceversa, sarà vincolata se nessuna di queste determinazioni è rimessa all'amministrazione, che nel suo comportamento sarà totalmente guidata dal dettato normativo.¹⁰⁴ Così, se una norma in materia di appalti assegna all'amministrazione il potere di stabilire che essa "può" escludere le offerte se non le considera valide, questo significa che la stessa legge assegna all'amministrazione la possibilità di scegliere tra più comportamenti (l'accettazione, la contestazione o il respingimento di un'offerta eccessivamente bassa) e la decisione sarà basata, a seguito di un contraddittorio, su una ponderazione di interessi (ad es. è più opportuno effettuare il lavoro a un costo basso ma con tempi più dilatati oppure sono preferibili maggiori garanzie di rispetto dei tempi stabiliti a fronte di un prezzo più alto?).

Accanto alla discrezionalità amministrativa propriamente detta, la dottrina considera anche la c.d. discrezionalità tecnica,¹⁰⁵ indicante lo spazio di apprezzamento proprio di scelte che non richiedono una ponderazione di interessi, ma hanno riguardo solo all'esecuzione materiale della legge

¹⁰¹ L'articolo in esame dispone: "ogni provvedimento amministrativo, compresi quelli concernenti l'organizzazione amministrativa, lo svolgimento dei pubblici concorsi ed il personale, deve essere motivato, salvo che nelle ipotesi previste dal comma 2. La motivazione deve indicare i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione dell'amministrazione, in relazione alle risultanze dell'istruttoria".

¹⁰² A. MASUCCI, *L'atto...*, cit, p. 101.

¹⁰³ A. MASUCCI, *L'atto...*, cit, p. 31, sottolinea le differenze tra concetti giuridici indeterminati e poteri discrezionali: in entrambi i casi si richiede all'amministrazione un apprezzamento che il legislatore ha ritenuto di non dover fissare nell'atto normativo, ma nel caso dei concetti indeterminati si tratta di attribuire un significato preciso ad un termine generico, e quindi di valutare quali fattispecie concrete siano riconducibili ad una fattispecie normativa indeterminata, compiendo quindi essenzialmente un'operazione interpretativa della norma giuridica e di qualificazione del caso concreto. Il caso della discrezionalità amministrativa è invece ben diverso, perché qui la norma conferisce un potere all'amministrazione, il cui contenuto consiste nella scelta tra diversi atti amministrativi da emanare, per cui non è in questione l'interpretazione della norma, ma il margine di libertà di comportamento da essa espressamente stabilito.

¹⁰⁴ Dal punto di vista strutturale si può osservare che le norme che assegnano margini di discrezionalità amministrativa sono normalmente riconoscibili dall'uso del verbo "potere" o espressioni affini, che conferiscono esplicitamente un potere, una facoltà, o in ogni caso un comportamento libero. Cfr. D. DE PRETIS, *Valutazione...*, cit., p. 25, la quale afferma che "laddove la legge utilizzi formule come «deve», «non può», «è tenuta a», è escluso che possa trattarsi di discrezionalità, considerato che l'amministrazione è obbligata a tenere un certo comportamento".

¹⁰⁵ Interessanti considerazioni in M. NATOLI, *Ambiti di operatività...*, cit., pp. 712-730.

attraverso cognizioni scientifiche, tecniche o artistiche.¹⁰⁶ Naturalmente non sono riconducibili a discrezionalità tecnica quei concetti giuridici indeterminati che richiamano giudizi di valore (come “bellezza” o “giusto prezzo”) non riferibili al dominio delle scienze o della tecnica.¹⁰⁷

4. L’atto amministrativo elettronico discrezionale: appunti per una ricostruzione

L’idea qui accennata di discrezionalità è considerata inconciliabile, per buona parte degli Autori, con il concetto di automazione informatica, perché la possibilità che un elaboratore elettronico sia in grado di compiere delle “scelte” (tanto più se basate su una “ponderazione di interessi”) non è normalmente rapportabile alla rigidità e alla predeterminazione logico-razionale che ne governano il comportamento:¹⁰⁸ al massimo la non prevedibilità offerta dal computer sarà data dalla sua velocità di ragionamento (quando deve elaborare un algoritmo complicato), ma questa non costituisce una autentica libertà d’azione.

In questo senso, l’attività dell’elaboratore è sempre da considerarsi rigidamente vincolata dalle istruzioni inserite dall’uomo attraverso il programma informatico per questo, più specificamente, se una legge domanda all’amministrazione una valutazione discrezionale, questa non potrà essere eseguita dall’elaboratore, a meno che non si prenda in esame la possibilità di

¹⁰⁶ Così P. CARINGELLA, *Corso di diritto amministrativo*, Milano, 2005, p. 276. La discrezionalità tecnica si può avere tutte le volte che la legge espressamente rimette all’amministrazione una valutazione empirica, ma può rinvenirsi anche quando è la formulazione stessa della norma, per la genericità dei termini usati, a richiedere l’ausilio di nozioni scientifiche per poter essere eseguita, e dunque quando sono presenti concetti giuridici indeterminati. Cfr. anche M. S. GIANNINI, *Istituzioni di diritto amministrativo*, Milano, 2000, p. 269, che delinea con la consueta chiarezza la possibilità che i concetti indeterminati (che implicano discrezionalità tecnica) e la discrezionalità amministrativa siano correlati ma nello stesso tempo rimangano distinti. Scrive l’esimo Autore: “...quali che siano le dimensioni dell’opinabilità, la c.d. discrezionalità tecnica non è mai discrezionalità amministrativa: è giudizio e manca la scelta. Questa semmai interverrà in un momento logicamente susseguente, allorché si dovrà decidere, p. es., se del progetto sbagliato occorre chiedere la correzione o il rifacimento o rifiutarlo o commettere nuova progettazione ad altri. [...] Si vuol dire cioè che in molti casi la discrezionalità amministrativa si radica sui giudizi della discrezionalità tecnica, ma resta da essa comunque distinta, ed è da essa solo relativamente condizionata: basti considerare le evenienze nelle quali il giudizio tecnico consiglierebbe una certa maniera di provvedere, e l’autorità decide invece di astenersi dall’intervenire o di adottare un provvedimento perché reputa preponderanti altri interessi...”.

¹⁰⁷ Per U. FANTIGROSSI, *Automazione...*, p. 70, “...la precisione della norma e conseguentemente il carattere vincolato dell’attività sono ritenuti sussistenti anche quando il significato o la portata della disposizione legislativa richieda comunque in sede di applicazione un’attività intellettuale da svolgersi sulla base di criteri non solo giuridici ma anche tecnici...”. In definitiva la norma prevede un comportamento non discrezionale dell’amministrazione, ma si esprime con concetti giuridici indeterminati. La legge quindi in questo caso non assegna una libertà di comportamento, bensì una libertà di interpretazione del proprio testo.

¹⁰⁸ Per questa opinione cfr. G. CARIDI, *Informatica giuridica e procedimenti amministrativi*, Milano, 1983, pp. 145 ss.; B. SELLERI, *Gli atti amministrativi in forma elettronica*, in *Dir. soc.*, n. 1, 1982; E. GIANNANTONIO, *Manuale di informatica giuridica*, Milano, 1998, p. 564; M. MINERVA, *L’attività...*, cit., p. 1304 e, in parte per quanto vedremo nel testo, A. MASUCCI, *L’atto...*, cit., p. 222.

“trasformarla” in una scelta vincolata, fissando dei parametri oggettivi in base ai quali deve essere assunta la decisione.

In altre parole, automatizzare una scelta discrezionale significa necessariamente poterla ricondurre ad una quantità finita di alternative e quindi ad un comportamento tutto sommato implicitamente vincolato.¹⁰⁹ Anzi, quanto detto è conforme ad un ormai consolidato orientamento giurisprudenziale e dottrinale, nato soprattutto per questioni di giustificazione motivazionale ma qui perfettamente richiamabile. Ad esempio, in tema di aggiudicazione dei contratti della Pubblica Amministrazione, il Consiglio di Stato ha affermato che il sistema della trattativa privata, che copre l'area residuale che va oltre l'asta pubblica e la licitazione privata (le quali, al contrario, sono chiaramente delimitate sotto il profilo procedurale) consente la massima libertà delle forme e attribuisce un'ampia potestà discrezionale all'Amministrazione, la quale, appunto, ben può autolimitarsi, ponendo condizioni procedurali che essa è tenuta a rispettare e la cui osservanza può essere fatta valere in sede di sindacato di legittimità.¹¹⁰

Da un punto di vista legislativo, invece, la legittimità dell'autolimitazione a mezzo di criteri predeterminati ha trovato una espressa affermazione proprio con l'emanazione della richiamata legge 7 agosto 1990 n. 241, la quale all'art. 12 stabilisce che *"la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati sono subordinate alla predeterminazione ed alla pubblicazione da parte delle amministrazioni precedenti, nelle forme previste dai rispettivi ordinamenti, dei criteri e delle modalità cui le amministrazioni stesse devono attenersi"*.¹¹¹

Sembra, quindi, del tutto acquisito al nostro ordinamento che l'autolimitazione della discrezionalità, a mezzo di provvedimenti generali che anticipano parzialmente le scelte predeterminandole in linea di massima, non è solo legittima ma, per talune ipotesi, addirittura doverosa. E allora torna in ballo la possibilità di configurare atti amministrativi elettronici discrezionali, i quali, a ben guardare, sono tali solo da un punto di vista superficiale e descrittivo, essendo in realtà anch'essi fondamentalmente vincolati.¹¹²

Ovviamente va da sé, per quanto fin qui sostenuto e al contrario, che se un ostacolo all'emissione di atti amministrativi automatici è costituito dalla presenza di spazi di discrezionalità amministrativa, nel momento in cui una

¹⁰⁹ Ritengono possibile l'automazione informatica anche in riferimento agli atti amministrativi discrezionali A. RAVALLI, *Atti amministrativi emanati mediante sistemi informatici: problematiche relative alla tutela giurisdizionale*, in *Trib. amm. reg.*, n. 2, Roma, 1989, pp. 261 ss. e V. BUSCEMA, *Discrezionalità amministrativa e reti neurali artificiali*, in *Foro amm.*, n. 2-3, 1993, p. 620.

¹¹⁰ La sentenza storica in tal senso è data da C.d.S., Sez. V, n. 27/1977. Da ultimo si veda la sentenza C.d.S. n. 2713/2005.

¹¹¹ Si può affermare che, nel caso in cui l'Amministrazione si sia autolimitata sull'*an* e non sul *quomodo* dell'esercizio di un proprio potere, essa è tenuta ad emettere un provvedimento esplicito, anche se di contenuto negativo, sì da consentire all'interessato di avere cognizione delle ragioni poste a fondamento dello stesso.

¹¹² Cfr. S. PUDDO, *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, Napoli, 2006.

determinata procedura sia totalmente vincolata essa potrà sicuramente essere affidata all'elaboratore. In questi casi, infatti, la legge prevede in modo perentorio e inderogabile i passaggi che dovranno essere seguiti per la sua attuazione, senza offrire margini di scelta tra opzioni diverse. Naturalmente, anche l'interpretazione della norma deve essere priva di margini di apprezzamento soggettivo: così, se si pensa al sistema di aggiudicazione del bando di gara nel fenomeno degli appalti pubblici *on-line* (*e-procurement*), la valutazione dell'offerta economica più vantaggiosa presuppone dei giudizi altamente discrezionali; in questi casi, infatti, l'amministrazione nella scelta del vincitore deve tenere conto di diversi fattori, di cui i più importanti sono il prezzo, il termine di esecuzione, il costo di utilizzazione, il rendimento ed il valore tecnico dell'opera.¹¹³ È evidente che in questa situazione non è possibile tipizzare tutti i casi possibili, senza considerare che la prefigurazione anticipata di un numero pur alto, ma sempre limitato, di ipotetiche fattispecie irrigidirebbe la procedura in modo ingiustificato, ostacolando proprio l'imparzialità e il buon andamento dell'amministrazione al cui principio è preordinato l'uso del sistema informatico.¹¹⁴

Dovendo, quindi, individuare e delimitare l'ambito dell'attività amministrativa totalmente vincolata,¹¹⁵ si possono distinguere i provvedimenti amministrativi in atti negoziali e in accertamenti costitutivi:¹¹⁶ mentre nei primi è lasciato sempre uno spazio di discrezionalità all'autorità amministrativa, nei secondi è prevista solo un'attività di accertamento della sussistenza dei requisiti previsti dalla legge, in presenza dei quali l'emissione

¹¹³ Cfr. S. CAMBRONE - A. TARMASSO, voce *Appalti pubblici (diritto comunitario)*, *Enc. Dir.*, Agg. III, 2002, p. 148, i quali riportano una sentenza della Corte di Giustizia della Comunità Europea che indica chiaramente come discrezionale il metodo di aggiudicazione dell'offerta più vantaggiosa: "l'aggiudicazione di un contratto di fornitura in base al criterio dell'offerta economicamente più vantaggiosa presuppone che l'amministrazione aggiudicatrice possa adottare una decisione discrezionale in base ai criteri qualitativi e quantitativi variabili a seconda del contratto e non sia vincolata unicamente dal criterio quantitativo della media delle offerte presentate". La sentenza è del 28 marzo 1985, causa 274/83 ("Commissione contro Repubblica Italiana"). Sull'*e-procurement* si veda da ultimo G. CALABRIA, *L' e-Procurement nella pubblica amministrazione italiana*, Milano, 2005.

¹¹⁴ Una possibile soluzione che è stata avanzata dalla dottrina di fronte a questi problemi consiste nella possibilità di utilizzare l'elaboratore solo quando la decisione è inquadrabile nei parametri precostituiti, mentre, nei casi in cui si presenta una situazione nuova che il programma non è in grado di qualificare, si emetterà un provvedimento tradizionale, non ad elaborazione elettronica. Nello stesso momento si dovrà provvedere all'aggiornamento del *software*, inserendo il caso in questione nella memoria del calcolatore, in modo tale che le future fattispecie analoghe possano essere trattate automaticamente. Cfr. U. FANTIGROSSI, *Automazione...*, cit., p. 94. Questa ipotesi è esclusa da altra dottrina, che mette in evidenza le difficoltà tecniche e gli alti costi di aggiornamento dei programmi informatici, che allo stato attuale sono difficilmente modificabili, impedendo l'automazione delle scelte discrezionali a media e alta complessità. Così A. MASUCCI, *L'atto...*, cit., p. 38.

¹¹⁵ In realtà la dottrina tende a "relativizzare" i concetti del discrezionale e del vincolante, perché è difficile che un procedimento possa essere del tutto vincolato e, al contrario, che l'azione stessa sia del tutto discrezionale: così B. G. MATTARELLA, *Il provvedimento...*, cit., p. 876 e A. G. OROFINO, *La patologia...*, cit., p. 2268 che richiama l'insegnamento di M. S. GIANNINI, *l'interpretazione dell'atto amministrativo*, Milano, 1939, ad opinione del quale si ha attività totalmente vincolata quando contemporaneamente la norma dispone in ordine al contenuto dell'atto, a quando emanarlo e a come debba essere formato, concludendo che tale evenienza costituisce un caso eccezionale.

¹¹⁶ Cfr. M.S. GIANNINI, *Istituzioni...*, cit., p. 78.

del provvedimento è un atto dovuto. Un esempio di accertamento costitutivo nell'ambito dell'informatica giuridica è dato dall'attività di certificazione offerta da una Certification Authority (CA) per la firma elettronica qualificata: se un cittadino presenta la domanda con allegata la documentazione necessaria, l'ente certificante deve procedere all'iscrizione nelle forme, nei modi e nei tempi che la legge prescrive, predisponendo il relativo certificato.¹¹⁷ Tutte le operazioni di questo tipo possono già essere svolte nella loro interezza dall'elaboratore elettronico, senza alcuna difficoltà né di ordine pratico, né di natura giuridica.

Anzi, secondo l'orientamento pressoché unanime della dottrina,¹¹⁸ l'automazione dell'attività vincolata può apportare solo benefici all'attività amministrativa in termini di imparzialità e di buon andamento. In questi casi, infatti, si ottiene in primo luogo la certezza di un'assoluta uguaglianza di trattamento dei cittadini, poiché vengono meno favoritismi fondati sul soprassedere a mancanze nei requisiti prescritti; sono inoltre esclusi gli errori dovuti a semplice distrazione dei funzionari incaricati (particolarmente frequenti in questo tipo d'attività, spesso monotone e ripetitive); infine, la velocità di elaborazione del computer permette di accorciare notevolmente i tempi di attesa per ottenere la risposta alle istanze presentate, che spesso potrà essere immediata. A tutto ciò si aggiunga il fatto che i pubblici uffici si potranno liberare dall'incombenza degli adempimenti ordinari meramente formali, che sottraggono oggi una parte assai rilevante delle risorse disponibili, e potranno invece indirizzare il personale umano in mansioni creative e in compiti che richiedano effettive valutazioni attente e puntuali. Ne consegue probabilmente una maggiore responsabilizzazione di tutto il personale, ma anche un lavoro più gratificante per i dipendenti e una conseguente maggiore produttività dell'attività amministrativa nel suo complesso.¹¹⁹

Al contrario degli atti vincolati, rimangono esclusi tutti quegli atti discrezionali in cui è difficile, se non impossibile, tipizzare in anticipo tutti i casi possibili: qui la rigidità legata alla pre-determinazione dei dati offerti dal programma informatico osta ad uno svolgimento corretto e legittimo dell'attività amministrativa. Questo è vero soprattutto se si tiene conto che il principio di imparzialità dell'attività amministrativa equivale a trattamento uguale di casi analoghi, ma anche a trattamento diverso di situazioni differenti.¹²⁰ Nelle decisioni più complesse, dunque, i vantaggi derivanti

¹¹⁷ Cfr. V. PEDACI, *Note intorno alle nozioni di potere discrezionale ed attività vincolata della Pubblica Amministrazione*, in *Nuova Rass.*, n. 21-22, 1996, p. 2079.

¹¹⁸ Cfr. A. USAI, *Le elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche*, Milano, 1994, pp. 77 ss., per il quale "l'attività vincolata, già allo stato dell'attuale sistema normativo, è legittimamente automatizzabile. Ciò in quanto non vi è nessuna autolimitazione della discrezionalità dell'organo. (...) Il sistema automatizzato fa le stesse identiche cose che farebbe il funzionario pubblico, con la differenza che mediante la procedura elettronica vi è uniformità, efficienza, versatilità". Cfr. anche U. FANTIGROSSI, *Automazione...*, cit., p. 75.

¹¹⁹ Cfr. G. TADDEI ELMI, *Corso di informatica giuridica*, Napoli, 2003, pp. 141 e 149.

¹²⁰ Cfr. U. FANTIGROSSI, *Automazione...*, cit., p. 95, e A. MASUCCI, *L'atto amministrativo...*, cit., p. 37.

dall'automazione non giustificano il sacrificio delle peculiarità dei singoli casi; e anche qualora fosse possibile tipizzare tutte le fattispecie ipotizzabili nel momento della stesura del *software*, quest'ultimo non sarebbe in grado di inquadrare e di qualificare situazioni completamente nuove che potrebbero presentarsi in seguito.

Allo stato presente, la soluzione da prendere in considerazione è allora solo quella dell'automazione delle scelte discrezionali che abbiano le caratteristiche di tipicità e ripetitività e la remissione di tutte le altre, a media e alta complessità, al funzionario "umano". Si configura così quella che è stata definita in dottrina un'automazione "a segmenti", che prevede, cioè, nell'ambito di uno stesso procedimento, un alternarsi di fasi in cui le decisioni sono affidate in parte al calcolatore e in parte al funzionario persona fisica.¹²¹

5. L'atto amministrativo elettronico discrezionale e i sistemi esperti: uno sguardo al futuro

Quanto si è affermato finora vale si riferisce essenzialmente all'informatica tradizionale. Ad essa si affiancano gli studi di informatica intesi a simulare il funzionamento della mente umana anche nei suoi meccanismi più "irrazionali" (come nelle scelte arbitrarie o nella creatività), vale a dire le ricerche sull'intelligenza artificiale (A.I.).¹²²

Con il termine di A.I. si considerano le applicazioni informatiche volte a permettere al calcolatore di svolgere gli stessi meccanismi cognitivi della mente umana.¹²³ Si tratta, in altre parole, di conferire all'elaboratore capacità come l'apprendimento, il compimento di scelte e, nelle ipotesi più avanzate, la creatività. Tali dibattiti, che sono tuttora in corso, non coinvolgono solo l'informatica, ma anche le scienze cognitive e, di riflesso, tutti gli ambiti della conoscenza umana, non ultime le discipline giuridiche. Le realizzazioni pratiche dell'intelligenza artificiale sono basate essenzialmente sulle cosiddette *reti neurali artificiali*, ossia sulla riproduzione al calcolatore delle

¹²¹ Cfr. G. CARIDI, *Informatica...*, cit., p. 100. L'Autore scrive che "il modello di descrizione può evidenziare che alcune parti del procedimento sono suscettibili, con vari livelli di difficoltà, di automazione, mentre altre, generalmente corrispondenti a quelle decisorie, non lo sono o non conviene che lo siano. In tal caso si può adottare un'automazione «a segmenti» in base alla quale la sequenza delle operazioni è sottoposta in alcune parti a controllo automatico, in altre, in corrispondenza di opportune interruzioni, segue il suo corso tradizionale, affidata all'esclusivo controllo umano". Cfr. anche A. MASUCCI, *L'atto...*, cit., p. 52, per cui l'automazione "a segmenti" non rappresenta l'eccezione bensì la norma negli attuali sistemi amministrativi, i quali stanno vedendo una crescita, e non una riduzione, delle attività discrezionali nella P.A.

¹²² Sull'argomento, oltre alla letteratura citata nel cap. I di questo lavoro, cfr. R. M. DI GIORGI, *L'intelligenza artificiale: teoria e applicazioni nel diritto*, in R. BORRUSO, *L'informatica...*, cit., pp. 185-236 e da ultimo P. L. LUCATUORTO, *Intelligenza artificiale e diritto: le applicazioni giuridiche dei sistemi esperti*, in *Cyberspazio e diritto*, n.2, 2006.

¹²³ Cfr. A. E. PÉREZ LUÑO, *Saggi di informatica giuridica*, Milano, 1998, p. 112, che fornisce la seguente definizione: "L'intelligenza artificiale si riferisce ad un insieme di attività informatiche che se fossero realizzate dall'uomo si considererebbero prodotto della sua intelligenza". Cfr. anche G. TADDEI ELMI, *Filosofia del diritto e informatica giuridica*, in D. A. LIMONE (a cura di), *Dalla giuritecnica all'informatica giuridica, studi dedicati a Vittorio Frosini*, Milano, 1995, p. 316, e pp. 341 ss.

connessioni tra i neuroni del cervello umano.¹²⁴ Caratteristiche dei calcolatori che operano con reti neurali artificiali sono la capacità di comprendere il linguaggio naturale, la possibilità di auto-perfezionarsi progressivamente a seguito dell'acquisizione di nuovi elementi e l'essere in grado di completare e interpolare informazioni frammentarie o incomplete.¹²⁵

Tra i programmi che è possibile realizzare per mezzo delle reti neurali artificiali sono oggi particolarmente studiati i c.d. *sistemi esperti*.¹²⁶ Si tratta di *software* in grado di riprodurre il comportamento che avrebbe un essere umano competente in una particolare materia, e quindi in grado di fornire le soluzioni ai problemi che si possono presentare in quel determinato ambito. La risposta ai problemi non è fornita, come avviene nell'informatica tradizionale, attraverso una rigida predeterminazione dei casi possibili e delle conseguenze ad essi associate (che, come si è già visto, impedisce al calcolatore di affrontare problemi "nuovi"), ma attraverso la capacità del calcolatore di apprendere le soluzioni da adottare mediante l'analisi di situazioni concrete.¹²⁷

Nel caso dell'emissione di provvedimenti amministrativi discrezionali, quindi, i sistemi esperti sarebbero in grado di elaborare nuove decisioni ricavando i criteri per la scelta dalla conoscenza delle deliberazioni precedenti. Ogni nuova fattispecie che è sottoposta al calcolatore è inoltre in grado di agire retroattivamente, modificando la base di conoscenza e fungendo da presupposto per le decisioni successive, migliorando costantemente l'attendibilità delle risposte dell'elaboratore.¹²⁸

Con riguardo alla loro adozione nell'ambito della P.A., si registrano in dottrina pareri discordanti.¹²⁹ Da una parte vi sono coloro che ne auspicano l'introduzione, sostenendo che si potrebbero in questo modo apportare anche all'attività discrezionale i vantaggi che già oggi si possono ottenere con l'informatica tradizionale per l'attività vincolata (imparzialità, buon

¹²⁴ Un interessante applicazione delle reti neurali all'ambito amministrativo è descritta da G. TERRACCIANO, *L'applicazione in campo giuridico delle reti neurali artificiali. Il programma «Giurinet»*, in *Trib. amm. reg.*, n. 12, pt. 2, 1998, pp. 497-509.

¹²⁵ Cfr. V. BUSCEMA, *Discrezionalità...*, cit., p. 624.

¹²⁶ Su tutti G. CARIDI, *Sistemi esperti e pubblica amministrazione*, in D. A. LIMONE, *Dalla giuritecnica...*, cit., pp. 105-126. Cfr. anche E. CORTELLINI - F. EUGENI, *Sistemi esperti*, in A. C. AMATO MANGIAMELI, *Parola chiave...*, cit., pp. 93-115.

¹²⁷ In termini tecnici, si può dire che il sistema esperto presuppone una *base di conoscenza*, data dall'insieme delle informazioni che costituiscono la "esperienza" del calcolatore, alle quali viene applicato un *motore inferenziale*, ossia un processo deduttivo che permette di trovare soluzioni a problemi *nuovi*, non previsti in anticipo, attraverso l' analogia con i casi già conosciuti. L'uso dei sistemi esperti presuppone quindi una fase di addestramento (*training*) della macchina, in cui le sono sottoposti i casi concreti associati alle relative soluzioni, alla quale segue una fase in cui il calcolatore, autonomamente, fornisce le risposte a problemi nuovi, sulla base della sua "esperienza": cfr. G. TERRACCIANO, *L'applicazione...*, cit., p. 498; A. PÉREZ LUÑO, *Saggi...*, cit., p. 128 e R. BORRUSO, *La legge...*, cit., p. 24.

¹²⁸ Per i problemi giuridici che i sistemi esperti comportano cfr. F. MACIOCE, *Un'ermeneutica per i sistemi esperti? Problemi e prospettive*, in A. C. AMATO MANGIAMELI, *Parola...*, cit., pp. 117-143.

¹²⁹ Sulle concrete applicazioni dei sistemi esperti nell'ambito dell'amministrazione cfr. G. CARIDI, *Corso elettronico di informatica giuridica*, Napoli, 2002.

andamento, compressione dei tempi, ecc..).¹³⁰ Dall'altra parte si hanno quelle posizioni, nettamente maggioritarie, che non vedono nell'introduzione dei sistemi esperti le possibilità di un reale miglioramento dell'attività amministrativa.¹³¹ Le argomentazioni più frequentemente avanzate contro l'adozione dei sistemi esperti nell'amministrazione riguardano sostanzialmente il fatto che, benché molto più avanzati dei *software* tradizionali, anche i programmi basati sulle reti neurali artificiali sono comunque caratterizzati da una certa rigidità, "...da una impostazione riduzionistica che porta a trasporre su un piano deterministico anche quei processi mentali che in realtà sfuggono a qualunque possibilità di razionalizzazione...".¹³² Inoltre, se non adeguatamente motivate, le scelte in tal senso intraprese rischiano di essere tutt'altro che trasparenti e controllabili ai fini di legittimità formale e sostanziale.

Un dato su cui invece la dottrina maggioritaria si trova in accordo è che, se i sistemi esperti non possono essere gli esecutori ultimi di provvedimenti discrezionali ad alta complessità, possono comunque svolgere una funzione di ausilio nell'assunzione delle decisioni, diventando in una certa misura i nuovi "consulenti" dei funzionari amministrativi.¹³³ È da osservarsi, infatti, che nell'emanazione di un atto discrezionale il funzionario non è in grado di tener conto di tutta la casistica precedente in relazione a situazioni analoghe, della quale al contrario conosce solo una parte piuttosto ridotta.¹³⁴ E anche la stessa normativa da applicare o da tenere in considerazione spesso è molto vasta e frammentata in una miriade di leggi emesse in lunghissimi archi di tempo, che forse nessuno conosce nella loro interezza. Per queste ragioni, la presenza nell'ufficio di un sistema esperto che sia invece in grado di tenere in considerazione tutte queste informazioni sicuramente potrà fornire al funzionario stesso un validissimo aiuto, suggerendogli tutti gli elementi che possono concorrere all'assunzione della decisione più opportuna, che garantisca la migliore ponderazione degli interessi in ciascun caso concreto che si possa presentare.¹³⁵

¹³⁰ A. MASUCCI, *L'atto...*, cit., p. 35; USAI, *Le elaborazioni...*, cit., p. 64 ss., e pp. 82 ss.

¹³¹ Cfr. PÉREZ LUÑO, *Saggi...*, cit., pp. 128 ss., che riporta le principali ragioni addotte dalla dottrina contro la possibilità o, più spesso, contro l'opportunità di utilizzare i sistemi esperti nella P.A.

¹³² Così G. TADDEI ELMI, *Corso...*, cit., p. 108 il quale afferma altresì che "...tutta la tendenza culturale informatica, decisionale e legislativa, pur avendo delle indubbie implicazioni positive, rischia, se utilizzata in modo acritico e riduttivistico, di portare a situazioni di efficienza formale ma di povertà sostanziale...".

¹³³ Cfr. G. TERRACCIANO, *L'applicazione...*, cit., p. 509, B. SELLERI, *Gli atti...*, cit., p. 141.

¹³⁴ Cfr. R. BORRUSO, *La legge...*, cit., pp. 73-75; P. L. LUCATUORTO, *Intelligenza artificiale...*, cit. p. 1121.

¹³⁵ Cfr. R. BORRUSO, *La legge...*, cit., p. 77 ss. Il funzionario potrà anche disattendere il parere fornito dal computer, se la fattispecie in questione sfugge ad un possibile inquadramento informatico. In questo caso, comunque, la decisione assunta dall'amministrazione andrà ad aggiungersi alla base di conoscenza del sistema esperto, contribuendo al progressivo perfezionamento dell'attendibilità del programma.

PARTE II

Il diritto dell'informatica tra l'accesso e la tutela dei dati personali

CAPITOLO V

IMMA BARBATO

IL DIRITTO DI ACCESSO AI DOCUMENTI DELLA P.A. TRA PRIVACY E DIRITTO ALLA RISERVATEZZA

SOMMARIO: 1. La legge 31.12.1996 n. 675 sulla privacy e l'accesso alla documentazione della pubblica amministrazione. – 2. Il trattamento dei dati personali della P.A. e il diritto di accesso di cui alla legge 241/90. – 3. L'art. 27 della legge 675/96. – 4. Le responsabilità penali. – 5. I rapporti tra riservatezza ed accesso alla luce della normativa in tema di tutela dei dati personali. – 6. Il diritto di accesso dopo la legge 15/2005. – 7. Rapporti tra diritto di accesso e tutela della riservatezza. – 8. Conclusioni.

1. La legge sulla privacy.

La legge 675/96, c.d. legge sulla privacy, prevede una lunga serie di obblighi, sanzionati penalmente, a carico di chi si trovi a gestire raccolte di informazioni relative a terzi.

A tal proposito, l'art. 1 lett. d) definisce la figura del *titolare* della raccolta di informazioni, qualificandolo come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente associazione o organismo cui competono le decisioni in ordine alle finalità ed alle modalità di trattamento dei dati personali.

Dalla portata vastissima della definizione, si può dire che praticamente tutti i soggetti giuridici, e cioè i centri di imputazione di interessi dell'ordinamento giuridico, risultano essere sottoposti, per lo meno in qualità di *titolari*, all'applicazione della legge 675/96, purché ad essi spetti un potere di gestione di dati personali altrui.

Per fare qualche esempio, saranno tenuti ai vari adempimenti previsti le società commerciali, gli studi professionali, le imprese di ogni dimensione ed i lavoratori autonomi; in generale, tutti i soggetti, e quindi anche le pubbliche amministrazioni, che dispongano di registrazioni su carta o su computer di dati relativi a terzi. I terzi in questione vengono definiti *interessati*.

Sempre infatti all'art. 1, questa volta alla lettera f), si definisce l'*interessato* come la persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali. Per inciso, si noti che non occorre la personalità giuridica per rientrare nell'ambito definitorio.

Anche a questo proposito, la categoria soggettiva degli interessati risulta vastissima, rientrandovi tutti i soggetti cui, direttamente o anche solo indirettamente, si riferisca l'archivio cartaceo o elettronico.

Passando ora al campo oggettivo di applicazione, si consideri l'art. 1, paragrafo 2, laddove offre, oltre alle nozioni di banca dati, dato personale, comunicazione e diffusione, anche una definizione di *trattamento*, talmente

ampia e generica da comprendere ogni possibile attività relativa ai dati personali.

Costituisce, infatti, *trattamento* (art.1 lett. b) qualunque operazione o complesso di operazioni svolti con o senza l'ausilio di mezzi elettronici o comunque autorizzati o concernenti la raccolta, la conservazione, l'elaborazione, la modificazione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione ed, infine, la distruzione dati.

2. Il trattamento dei dati personali della P.A. e il diritto di accesso di cui alla legge 241/90.

Ogni amministrazione detiene una più o meno copiosa serie di dati relativi a persone fisiche, giuridiche o ad enti non conosciuti, comunemente in archivi documentali oppure in banche dati elettroniche.

Dato che le pubbliche amministrazioni rientrano nella nozione di *titolare*, si applicherà loro la legge 675/96 quando operazioni sulle raccolte di documenti o sugli schedari computerizzati.

Sempre in ordine all'attività della p.a., l'art. 22 della legge 7 agosto 1990 n. 241, come noto, prevede che è riconosciuto a chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti, il diritto di accesso ai documenti amministrativi.

Ai sensi del successivo II comma, è considerato documento amministrativo ogni rappresentazione grafica del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, comunque, utilizzati ai fini dell'attività amministrativa.

L'unico requisito posto dalla legge per accedere ai documenti della p.a., è che il richiedente dimostri di essere portatore di un interesse giuridicamente rilevante.

In via d'interpretazione estensiva, è stata pure riconosciuta la rilevanza dell'interesse a visionare gli atti procedimentali da parte dei destinatari anche solo indiretti del futuro provvedimento. Infine, è stata riconosciuta la rilevanza dell'interesse anche di chi non si trovi coinvolto affatto in un procedimento amministrativo in corso, ma semplicemente sia portatore di interessi di carattere personale, quali quello scientifico e di ricerca.

Le attività della p.a. strumentali al diritto di accesso previsto dalla legge 241/90, le attività cioè volte a garantire la visione dei documenti e l'ottenimento di copia di essi, sono di due tipi, una *interna* e l'altra *esterna*.

In primo luogo vi sono le attività consistenti nella raccolta e conservazione sistematica degli atti, nel loro raffronto e nell'estrazione della documentazione scelta; in secondo luogo si ha la consegna materiale dei documenti che, in tal modo, vengono messi a disposizione del privato.

Quando si compiono tali operazioni sui documenti, immancabilmente si verificano *trattamenti* di dati nel senso della legge sulla privacy, oltre che sui documenti, infatti, le operazioni suddette si svolgono anche sui dati personali

in essi eventualmente contenuti; le attività interne che servono per far accedere ai documenti, quindi, si possono qualificare come *trattamenti* ai sensi dell'art. 1 lett.b), legge 675/96.

Quanto alle attività che possiamo definire *esterne*, ai sensi dell'art.1 lett.g) della legge 675/96, il dare conoscenza dei dati personali ad uno o più soggetti determinati, diversi dall'interessato (e cioè a soggetti, quali il richiedente, diversi da quelli i cui dati sono contenuti nella documentazione), in qualunque forma, anche mediante la loro messa a disposizione o consultazione, è definita *comunicazione*.

La messa a disposizione dei dati e cioè, secondo la terminologia della legge sulla privacy, la *comunicazione* dei dati stessi, è sempre complementare all'esercizio del diritto d'accesso: è evidente infatti che nel mettere a disposizione del richiedente gli atti, la amministrazione non può contestualmente non comunicare i dati personali in essi contenuti.

Con riferimento a tutte le attività indicate, gli adempimenti cui sono tenute le p.a. in qualità di titolari di banche dati sono minori rispetto agli analoghi doveri posti in capo ai privati ed alle imprese (private e pubbliche), dal momento che le amministrazioni pubbliche non sono destinatarie che di una parte delle norme della legge 675/96.

In particolare, gli artt.11 e 20 della legge 675/96, che prevedono l'obbligatorietà del consenso preventivo dell'interessato, non si applicano alle pubbliche amministrazioni; per l'art. 10, infatti, è richiesto il consenso dell'interessato, solo quando il trattamento di dati personali avviene da parte di privati o di enti pubblici economici. Parallelamente, l'art.20, più specifico con riguardo a quel tipo di trattamento che consiste nella comunicazione o nella diffusione di dati personali, prevede che per tali attività sia necessario il *consenso* dell'interessato se esse siano svolte da parte di privati o enti pubblici economici, e non quindi dalle amministrazioni pubbliche generalmente intese. Per fare qualche esempio, il trattamento da parte degli enti territoriali (regioni, Comuni e Province), così come il trattamento da parte degli organi dello Stato, potrà essere compiuto a prescindere dal consenso degli interessati.

Per il resto, le amministrazioni pubbliche sia dello Stato che degli enti locali, saranno solo tenute, come qualunque altro *titolare*, agli ulteriori adempimenti previsti dalla legge 675/96: dovranno in particolare notificare al Garante l'informativa di cui all'art.7, dovranno nominare il proprio responsabile ai sensi dell'art. 8, dovranno trattare i dati personali secondo le modalità di cui all'art. 9 e, infine, dovranno comunicare agli *interessati* le informazioni di cui all'art.10.

Alle pubbliche amministrazioni sono parimenti applicabili gli artt. 22, 23, 24 e 28 della legge.

In conclusione, possiamo dire dunque che la p.a. è tenuta agli adempimenti che in genere competono a qualsiasi titolare, ma è esonerata dall'obbligo di ottenere il preventivo consenso degli interessati.

Sulla base degli artt. 11 e 20, infatti, il consenso del soggetto i cui dati vengono trattati non occorrerà né per le attività esterne né per le interne, e cioè né per i semplici trattamenti né per la comunicazione.

In sede di istanza di accesso alla documentazione della p.a., al richiedente non potrà, in altre parole, essere chiesto altro che, sulla base dell'art.22 della legge 241/90, di dimostrare che il suo interesse a vedere le carte è basato su esigenze giuridicamente rilevanti. Non è legittimo opporre la necessità del consenso degli interessati.

Occorre esaminare, poi, gli artt. 13 e 22 della legge 675/96, onde verificarne la compatibilità con il diritto di accesso ricopiuto dalla legge 241/90.

L'art.13 lett. g) della legge 675/96, prevede che in relazione al *trattamento* di dati personali, l'interessato ha diritto di opporsi, in tutto in parte, al *trattamento* dei dati personali che lo riguardano.

A differenza degli artt.11 e 20 sul consenso, la disposizione in esame si applica oltre che ai dati detenuti da privati o da enti pubblici economici, anche a quelli gestiti da tutte le amministrazioni pubbliche.

Essa riconosce agli *interessati* il diritto potestativo di bloccare i trattamenti sui loro dati personali. Si tratterà quindi di valutare se tale diritto di veto può anche essere esercitato per opporsi all'accesso di cui alla legge 241/90.

Si prenda poi in esame l'art. 22 sui cosiddetti *dati sensibili* (razza, opinioni politiche, convinzioni religiose etc..), esso dispone che il trattamento di dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espresse disposizioni di legge.

Per tali dati, il trattamento da parte della pubblica amministrazione deve ritenersi generalmente vietato, salvo appunto il caso che una legge lo autorizzi.

Gli interrogativi che nascono dagli artt. 13 e 22 sono quindi due:

- potrà una persona opporre il proprio veto all'accesso ai documenti che contengono i suoi dati in possesso della p.a.?
- sarà necessaria la legge d'autorizzazione di cui all'art. 22 perché si possa accedere ai documenti amministrativi contenenti dati sensibili?

La soluzione ai due quesiti può essere data sulla base di alcune semplici considerazioni.

In primo luogo, secondo l'art. 43 della legge 675/96, conformemente del resto all'art.27, restano ferme le disposizioni della legge 20 maggio 1970 n. 300 nonché, in quanto compatibili, le disposizioni della legge 5 giugno 1990 n. 135 e del D.lvo 6 settembre 1989 n. 322, nonché le vigenti norme in materia di accesso ai documenti amministrativi.

La norma suddetta sembra aver fatto salve, *sic et simpliciter*, tutte le norme della legge 241/90 e le relative norme d'attuazione.

Il dato letterale sembra prevedere chiaramente che, proprio con riguardo all'accesso, e cioè alla legge 241/90 e relativi regolamenti di

attuazione, i problemi di coordinamento con la legge sulla privacy debbano essere tranciati a monte.

La norma, del resto è facilmente comprensibile alla luce dell'autonomia concettuale della legge sull'accesso rispetto alla legge sulla privacy.

Come noto, la legge 241/90 costituisce una fonte attuativa dell'art. 97 Costituzione, in proposito basta leggere l'art. 22 comma 1 della legge 241/90, per constatare come tale legge sia stata emanata per perseguire la trasparenza dell'amministrazione e, quindi, per attuare i precetti costituzionali dell'imparzialità e del buon andamento dell'amministrazione.

La legge 241/90 presuppone insomma una ratio completamente autonoma rispetto alla legge sulla privacy, ratio che si manifesta in una disciplina speciale del trattamento dei documenti in possesso della p.a.

In proposito, l'art 43 ha fatto integralmente salve le regole sul diritto d'accesso, non per caso, ma in primo luogo per la autonomia delle regole poste dalla legge 241/90, regole basate su distinti presupposti costituzionali e volte ad assicurare la trasparenza della p.a. Ciò non significa che la legge 241/90, anche perseguendo obiettivi propri, si sia disinteressata della riservatezza delle persone.

In proposito, l'art. 24 lett. d) ha espressamente delegato il Governo ad emanare le norme per salvaguardare la riservatezza di terzi, persone, gruppi ed imprese, garantendo peraltro agli interessati la visione degli atti relativi ai procedimenti amministrativi, la cui conoscenza sia necessaria per curare o per difendere i loro interessi giuridici.

In osservanza della delega dell'art. 24, il Governo ha poi previsto, nel regolamento del 27.6.1992 n. 352 altre limitazioni al diritto d'accesso, sempre a garanzia base della riservatezza terzi.

Inoltre, questa volta in attuazione dell'art.24 IV comma,le singole amministrazioni hanno individuato le categorie di documenti sottratti all'accesso, ancora una volta, per tutelare il diritto alla riservatezza, dunque in conclusione si ritiene che l'art. 43 della legge 675/96 abbia stabilito la salvezza in toto della legge 241/90, da un lato perché tale legge presenta caratteri di specialità ed autonomia, ed in secondo luogo perché la tutela della privacy non è estranea alla legge 241/90, ma viene da essa garantita in maniera specifica, anche se adeguatamente alle esigenze di preservare la trasparenza dell'attività amministrativa.

Dobbiamo di conseguenza affermare come la legge 241/90 non sia intaccata dalle norme sulla privacy, come ha espresso di recente anche il T.A.R Abruzzo, sez. Pescara, con la sentenza 5.12.1997 n. 681.

Se si considera infatti il breve passaggio della pronuncia nel quale è stato chiarito come la norma di cui all'art. 43, comma 2, della legge 31.12.1996 n.65, in materia di tutela del trattamento dei dati personali, ha lasciato ferme le vigenti disposizioni in materia di accesso ai documenti amministrativi, se ne deve ricavare che il legislatore ha inteso far salva tutta la normativa vigente in ordine al diritto d'accesso, e ciò, in relazione ai rapporti

tra il diritto alla riservatezza ed i principi della trasparenza dell'attività amministrativa, di cui il *diritto di accesso* costituisce un corollario.

Sotto il profilo dei dati contenuti in documenti della p.a., se così è, le norme della legge 241/90 prevalgono sugli artt. 13 e 20 della legge 675/96, in particolare, l'accesso non potrà essere condizionato negativamente né dal veto eventualmente espresso dall'interessato né, in secondo luogo, dalla mancanza della speciale legge d'autorizzazione sui dati sensibili.

Tuttavia, siccome qualche autore, ha affacciato la possibilità che l'inciso "*in quanto compatibili*" contenuto nell'art. 43 possa significare che la legge 241/90 non sopravviva integralmente ma solo laddove compatibile con le nuove norme sulla privacy, si deve considerare:

- In primo luogo, dalla lettera dell'art. 43 sembra che l'inciso "*in quanto compatibili*" vada riferito solo alla legge 5 giugno n. 135 ed al D.lvo 6 settembre 1989 n. 322, e non anche alle disposizioni sull'accesso

- Inoltre, sia la legge n. 241 che la legge 675/96 garantiscono, come si può agevolmente ricavare rispettivamente dai loro articoli 24 e 1, e come già detto in precedenza, la riservatezza dei terzi, la prima legge in misura tale da non configgere con l'opposta esigenza della trasparenza amministrativa, la seconda in maniera generalizzata per tutti i titolari di trattamenti.

Le due leggi si pongono, perseguendo distinte finalità, in un rapporto di specialità.

La legge 241/90 costituisce in fatti un corpus normativo rivolto a disciplinare esclusivamente le situazioni particolari che consistono nei *trattamenti* funzionali all'esercizio del *diritto di accesso*.

Tali *trattamenti*, che come abbiamo detto sono necessari alla visione degli atti da parte dei privati, sono solo una parte dei *trattamenti* di cui si occupa in via generale la legge 675/96.

Ecco perché, anche in base a quanto disposto dall'art. 15 delle Preleggi al codice civile, in primo luogo per la particolarità della materia, la legge 241/90 si presenta come speciale rispetto alla legge sulla privacy e, come tale, non può considerarsi abrogata da quest'ultima.

Un secondo indice della specialità della legge 241/90 sta nel fatto che essa si rivolge unicamente alle attività di trattamento poste in essere dalla pubblica amministrazione mentre la legge 675/96 pone norme che valgono, tranne eccezioni, per tutti i soggetti giuridici.

Concludendo, la legge 241/90 sembra speciale rispetto alla legge 675/96 e quindi ad essa aggiuntiva, se le due normative possono convivere appunto perché regolano settori distinti, e quindi possiamo affermare che esse sono compatibili.

Ci informa a tal proposito la sentenza della Corte di Cassazione n. 1493/79 che le due normative sono incompatibili solo quando tra le leggi considerate vi sia una contraddizione tale da renderne impossibile la contemporanea applicazione.

Ne consegue che la disciplina del diritto di accesso non risulta essere stata modificata, nemmeno sotto i due profili dei dati sensibili e del diritto di

veto e pertanto la p.a. dovrà anche nei casi suddetti consentire l'accesso sempre che il richiedente dimostri di essere portatore di un interesse rilevante e sempre che l'accesso sia consentito dai regolamenti di attuazione della legge 241/90.

3. L'art.27 della legge 675/96

La considerazione secondo cui la legge n. 675/96 non ha introdotto modifiche o abrogazioni alla legge 241/90, risulta confermata anche dal dettato dell'art. 27 della legge 675/96 che dispone al I comma, che il *trattamento di dati personali da parte di soggetti pubblici, esclusi gli enti pubblici non economici, è consentito soltanto per lo svolgimento delle funzioni istituzionali nei limiti stabiliti dalle leggi e dai regolamenti*, e, al III comma, che *la comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o ad enti pubblici economici, sono ammesse solo se previste da norme di legge o di regolamento*.

A ben vedere, la norma di cui al I comma sopra riportato *non dice nulla di nuovo*, né in relazione al fatto che il trattamento risulta consentito *solo per lo svolgimento delle funzioni istituzionali* né quando richiama i limiti *stabiliti dalle leggi e dai regolamenti*.

Il richiamo alle funzioni istituzionali sembra superfluo, per la considerazione che ogni attività della pubblica amministrazione deve sempre e comunque muoversi all'interno delle funzioni istituzionali fissate dalle leggi. Altrettanto ultroneo appare il richiamo all'obbligatorio rispetto dei limiti imposti dalle leggi o dai regolamenti, poiché è ovvio che ogni *trattamento*, anche da parte della pubblica amministrazione, non può che avvenire conformemente a leggi o a regolamenti.

Il III comma introduce una disposizione più restrittiva rispetto al I comma poiché consente quella sottospecie di *trattamento* che consiste nella *comunicazione*, solo se tale *comunicazione* sia espressamente ammessa da specifiche leggi e regolamenti.

Al di là di questa sommaria analisi delle norme, quel che rileva è considerare che il *diritto d'accesso*, come disciplinato dalla l. 241/90 e relativi regolamenti, risulta comprensivo sia dei trattamenti di cui al I comma dell'art. 27, sia della *comunicazione* di cui al III comma dello stesso art.27, secondo quanto si è cercato di spiegare *supra*.

Ed allora, poiché la l. 241/90 attribuisce alla p.a. la *funzione* di garantire la trasparenza del proprio operato (anche consentendo l'accesso ai propri documenti a favore dei portatori di interessi rilevanti) e poiché la l. 241/90 e relativi regolamenti introducono una precisa disciplina del *diritto d'accesso* (che come detto si risolve in *comunicazione*), ne discende che l'art. 27 e la l. 241/90 sono perfettamente compatibili ed il rispetto della disciplina della l. 241/90 e dei relativi regolamenti assicurano anche il rispetto della l. 675/96.

4. Le responsabilità penali

L'art. 35 prevede che chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al *trattamento* di dati personali in violazione dell'art. 27 è punito con la reclusione fino a due anni o, se il fatto consiste nella *comunicazione o diffusione*, con la reclusione minima di tre mesi.

Il secondo comma dello stesso art. 35 prevede un'analogha sanzione penale per le ipotesi di *comunicazione o diffusione* dei dati personali, in violazione degli artt. 21, 22, 23, 24 e 28 comma 3 della legge.

Per il terzo comma, se dai fatti di reato deriva nocumento la reclusione è aumentata.

A tal proposito, si possono fare alcuni appunti di carattere generale: le norme suindicate rinviano, ai fini della qualificazione della condotta punibile e dei soggetti responsabili, alle definizioni contenute nell'art. 1 della l. 675/96. In conseguenza tali norme descrivono fattispecie di reato che non sembrano, a nostro avviso, sufficientemente determinate, tanto sotto il profilo della condotta punibile, che sotto il profilo dell'individuazione delle persone perseguibili.

Non mancheranno sicuramente, fin dai primi casi sottoposti alla giurisdizione penale, le questioni sulla insufficiente tassatività delle fattispecie incriminabili.

Per ora, in mancanza di una giurisprudenza che riconduca le norme suindicate nell'alveo del principio della tassatività delle norme penali, si è creata, un po' dappertutto, una vera e propria sindrome da *privacy*.

Anche la pubblica amministrazione, colta sicuramente di sorpresa da una legge complessa ed intricata, scarsamente coordinata con le norme amministrativistiche, in taluni casi ha iniziato con l'improvvisare un'applicazione della legge 675/96 in contrasto con le fonti del diritto amministrativo, ed in particolare con la legge 241/90.

Vediamo dunque come la l. 241/90 continua ad essere valida ed a disciplinare autonomamente l'accesso alla documentazione pubblica, dando pertanto applicazione corretta alla 241/90, nessun impiegato della p.a. potrà incorrere nelle sanzioni previste dalla l. 675/96.

L'unica cosa che dovrà fare, come sempre fino ad oggi, sarà quella di valutare la rilevanza giuridica dell'interesse di chi chiede di vedere i documenti, e conseguentemente consentire l'accesso nei limiti posti dalla legge 241/90 e dai relativi regolamenti d'attuazione (DPR 27.6.1992 n. 352) e gli altri regolamenti adottati dalle singole amministrazioni.

5. I rapporti tra riservatezza ed accesso alla luce della normativa in tema di tutela dei dati personali

A 15 anni dalla prima legge generale italiana sul procedimento amministrativo, la legge 241/90, il Parlamento ne ha approvato la riforma con la legge 11 febbraio 2005 n. 15.

Vengono inseriti tra i criteri generali dell'azione amministrativa la trasparenza (inserimento doveroso, visto che la legge 241 era nota a tutti come "legge sulla trasparenza" ma non veniva espressamente enunciata in essa) e l'osservanza dei principi dell'ordinamento comunitario (comma 1), che devono essere rispettati anche dai concessionari dei pubblici servizi (comma 1-ter).

La trasparenza è un mezzo di attuazione della democrazia, intesa secondo un'efficace immagine di Bobbio come "regime del potere invisibile".

Al principio di trasparenza si connettono sia l'accesso sia il principio di partecipazione e l'obbligo di motivazione.

Il rispetto dell'ordinamento comunitario è già sancito nell'art. 117, co. 1 Cost. novellato, laddove si precisa che esso è un vincolo alla potestà legislativa dello Stato e delle regioni.

Giova ricordare che, a partire dalla storica sentenza della Corte costituzionale n. 170 del 1984, le norme comunitarie produttive di effetti diretti (regolamenti, direttive *self-executing* e sentenze interpretative della Corte di Giustizia) operano con efficacia immediata nel nostro ordinamento, indipendentemente dalle leggi precedenti o successive, che vengono semplicemente "non applicate" dai giudici nazionali.

È l'art. 11 della Costituzione che funge da "trasformatore permanente" delle norme comunitarie in norme interne, in quanto l'ordinamento comunitario è un insieme di norme ed istituzioni che mira a rafforzare la pace e la giustizia fra le nazioni e pertanto può apportare quelle "limitazioni di sovranità" al nostro sistema costituzionale in materia di fonti del diritto.

6. Il diritto di accesso dopo la legge 15/2005

La legge 11.2.2005 n. 15, innovando profondamente la legge generale sul procedimento amministrativo n.241/90, ha dettato una disciplina più organica e completa in materia di accesso ai documenti, disciplinato dal capo V agli artt. 22 e seg.

L'art. 22 come novellato dalla legge n.15/2005 alla lett. a) del comma 1 si preoccupa, a differenza della normativa precedente, di definire il diritto d'accesso, inteso come il diritto degli interessati di prendere visione e di estrarre copia dei documenti amministrativi.

Il diritto di accesso in questione è il c.d. accesso conoscitivo (o informativo) e va distinto dal c.d. accesso partecipativo disciplinato dal precedente art. 10 della legge 241/90, ove l'accesso partecipativo è il diritto dei destinatari della comunicazione dell'avvio del procedimento di prendere visione degli atti dello stesso al fine di presentarne all'interno memorie e documenti.

Il fondamento giuridico del diritto d'accesso (conoscitivo) va individuato nel principio di trasparenza dell'attività amministrativa e più a monte negli artt. 97 e 98 Cost. ove si enuncia il principio di buon andamento dei pubblici uffici (parte della dottrina ha invece collegato il diritto d'accesso al diritto di informazione, garantito dall'art. 21 Cost.).

La stessa legge 15/2005 contiene in proposito un'importante enunciazione di principio, laddove innovando l'art. 22 della legge n. 241/90, prevede che l'accesso ai documenti, attese le sue rilevanti finalità di pubblico interesse, costituisce un principio generale dell'attività amministrativa, finalizzato a favorire la partecipazione dei privati e ad assicurare l'imparzialità e trasparenza dell'azione amministrativa.

Poiché il diritto di accesso, prosegue la norma, attiene ai "livelli essenziali delle prestazioni concernenti i diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale", il relativo fondamento può essere rinvenuto anche nell'art. 117 co. 2 lett. m) della Cost., espressamente richiamato dal nuovo art.22.

7. Rapporti tra diritto di accesso e tutela della riservatezza.

In tema di accesso si è prospettato il possibile conflitto di interessi tra la tutela accordata dall'ordinamento al relativo diritto e quella riconosciuta al diritto alla riservatezza, allorché la richiesta di accesso riguardi documenti contenenti notizie su soggetti estranei alla P.A. (individui o imprese) e vengano in rilievo notizie intime di terzi che, pur se conosciute dalla P.A., non dovrebbero essere accessibili ai terzi.

Partendo dall'esame della soluzione scelta dall'art. 24 della legge 241/90, la prevalenza del diritto di accesso era ancorata a due condizioni:

- 1) L'accesso deve mirare alla tutela di interessi giuridicamente rilevanti;
- 2) Il diritto d'accesso deve inoltre limitarsi alla sola possibilità di prendere visione degli atti (restando escluso il rilascio di copia).

L'art. 8 del d.p.r. 352/92 ribadiva tale impostazione, aggiungendo che, fuori dai suddetti limiti, doveva prevalere il diritto alla riservatezza.

Il sopravvento della legge n.675/1996, in tema di trattamento dei dati personali, innescò una serie di problemi:

- L'art. 43 dispose che "restano ferme le norme vigenti in tema di accesso ai documenti";
- L'art. 22 sottopose il trattamento (e quindi la divulgazione) dei c.d. dati sensibili a speciali limitazioni, disponendo che il trattamento dei dati sensibili da parte degli enti pubblici è consentito solo nei casi stabiliti dalla legge che deve evidenziare le finalità di pubblico interesse, le operazioni eseguibili nonché i dati trattabili;
- Infine l'art. 27 in base al quale la comunicazione e diffusione da soggetti pubblici a privati di dati personali (non sensibili) è consentita nei casi previsti dalla legge o regolamento .

La soluzione interpretativa proposta dal Consiglio di Stato con la decisione n.59/99 prese il nome di “doppio binario”:

- Quanto ai dati comuni (ossia non sensibili), l’accesso deve ritenersi consentito solo per la tutela di interessi rilevanti ed è limitato alla presa visione del documento (cfr. art. 27 che rinvia ai casi previsti dalla legge, ossia all’art. 24 della legge 241/90)

- Quanto ai dati c.d. sensibili, l’art. 22 consente l’accesso solo se lo preveda una specifica disposizione di legge che evidenzi le finalità di pubblico interesse, le operazioni eseguibili ed i dati trattabili.

Il decreto legislativo n. 135/99 è tuttavia intervenuto a modificare l’impostazione della legge n. 675/99 circa il trattamento e l’accesso dei dati sensibili. In base al nuovo art. 22 comma 3 e 3bis della legge 675 (come modificati dal d.lgs. n. 135/99) il trattamento dei dati sensibili da parte della p.a. può avvenire nei seguenti casi ed attraverso le seguenti modalità:

1) In caso di espressa previsione di legge che specifichi i dati trattabili, le operazioni eseguibili e le finalità di pubblico interesse ritenute prevalenti.

2) In mancanza di legge e nelle more della sua adozione, la P.A. può demandare al Garante di individuare quali tra le attività debbono considerarsi di rilevante interesse pubblico e come tali consentire il trattamento dei dati sensibili.

3) Quando una legge determini le finalità di rilevante interesse pubblico ma non specifica il tipo di operazioni eseguibili o i dati trattabili, sarà la singola P.A. interessata ad effettuare l’eventuale operazione integrativa per poi passare a compiere il trattamento dei dati.

Ciò posto, va rilevato, con specifico riferimento al diritto d’accesso, che l’art. 16 del decreto in commento qualifica l’accesso (*rectius*: il trattamento mediante ostensione) quale attività di rilevante interesse pubblico, con la conseguenza che viene a cadere il primo limite al trattamento mediante ostensione dei dati sensibili essendovi una legge (appunto l’art. 16 citato) che esprime le finalità di pubblico interesse sottese al diritto d’accesso.

Tale sistema appare confermato dal d.lgs. n. 196/2003 (nuovo codice della *privacy*) il cui art. 59 dispone che il diritto di accesso ai documenti contenenti dati personali o sensibili e le operazioni di trattamento eseguibili in conseguenza di una domanda di accesso restano disciplinati dalla legge n. 241/90 e dalle altre disposizioni in materia, riconfermando, inoltre, che le attività in oggetto (accesso e trattamento) si considerano di rilevante interesse pubblico.

Ulteriore problema si è posto, infine, per i dati c.d. supersensibili, ossia idonei a rilevare lo stato di salute o la vita sessuale dell’individuo.

L’art. 16 comma 2 del d.lgs. n. 135/99 ha stabilito che in tal caso il trattamento è consentito solo se il diritto contrapposto:

- Deve essere difeso in giudizio civile o amministrativo (se, cioè, il trattamento è funzionale alla difesa di un diritto in giudizio);

- È di rango almeno pari a quello (alla riservatezza) dell’interessato, in un’ottica di bilanciamento di interessi.

Tale impostazione è stata confermata e precisata dall'art. 60 del nuovo codice della *privacy* (196/2003) che:

- Estende la previsione (oltre che al trattamento) al diritto d'accesso;
- Precisa che il diritto del controinteressato deve essere o di pari rango oppure consistere in un diritto della personalità ovvero in un altro diritto o libertà fondamentale ed inviolabile.

La legge n. 15/2005 costituisce il punto di arrivo del lungo percorso evolutivo sopra esaminato.

L'art. 16, nel sostituire l'art. 24 della legge 241/90, dopo aver statuito che deve essere comunque garantito il diritto d'accesso ai documenti la cui conoscenza è necessaria per curare o difendere i propri interessi giuridici, ha espressamente disposto che:

- Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito "nei limiti in cui sia strettamente indispensabile"
- Nel caso di dati c.d. supersensibili l'accesso è consentito nei limiti previsti dall'art. 6 del nuovo codice della *privacy*.

8. Conclusioni

Possiamo dunque dire che il modello fin qui delineato di P.A. dalla riforma segna il passaggio da un principio di garanzia formale ad un principio di garanzia sostanziale dell'azione amministrativa.

L'idea di fondo ma anche la "grande scommessa" da vincere, è rafforzare l'efficienza attraverso strumenti di tutela del cittadino, rendendo più economica ed efficace l'azione amministrativa.

L'efficienza del sistema pubblico è diventata una condizione indispensabile per garantire risultati economici in un Paese che voglia essere veramente moderno e pronto per le sfide epocali che ci riserva il Terzo millennio.

Con gli obiettivi della speditezza, partecipazione e trasparenza, si contribuisce certamente a semplificare l'azione amministrativa migliorando la qualità delle prestazioni a favore del cittadino, ma non bastano leggi generali, se non si rivedono i meccanismi costituzionali: è anche il nuovo impianto costituzionale, che, essendo fonte di conflitti continui tra Stato ed Autonomie, contribuisce a rallentare l'azione amministrativa.

Infatti la razionalità e l'efficienza della P.A. si perseguono non solo nel rapporto evolutivo Istituzioni-cittadini ma anche nel corretto rapporto tra le Istituzioni medesime, che, in assenza di regole chiare, si inceppa spesso, a causa di norme confuse e complesse, con buona pace, purtroppo, delle certezze del diritto.

CAPITOLO VI

GIULIANA ASTARITA

LA TUTELA DEI DATI PERSONALI NELLE ATTIVITA' PRODUTTIVE

SOMMARIO: 1. Premessa. – 2. Il diritto alla tutela dei dati personali e l'attività d'impresa.. – 2.1. La firma digitale. – 2.2. La tutela dei dati personali nel rapporto di lavoro. – 2.3. La tutela dei dati personali e la concorrenza. – 2.4. La tutela dei dati personali ed il rapporto con i consumatori e gli utenti. L'attività di *marketing* e lo *spamming*. – 3. I costi della tutela dei dati personali. – 4. La tutela dei dati personali come qualità e risorsa aziendale. – 5. conclusioni.

1. Premessa.

Nel processo di innovazione tecnologica, in una società “a cambiamento velocissimo”¹³⁶ com'è quella attuale, che moltiplica il trattamento dei dati, il sistema economico ed imprenditoriale assume un ruolo centrale.

Il progresso tecnologico favorisce lo sviluppo di meccanismi di comunicazione un tempo impensabili, ove è consentito quasi annullare le distanze dei trasferimenti delle merci e dei servizi, dei capitali, delle persone. I tempi di realizzazione delle scelte sono ridotti e ciò incide sulle modalità di produzione e di distribuzione dei beni.

Ciò porta a ritenere che “...una generale normativa sulla protezione dei dati personali (sia) davvero il crocevia verso il quale convergono i percorsi di sviluppo della società contemporanea..”¹³⁷

L'analisi delle conseguenze di queste innovazioni e dei possibili percorsi di sviluppo non è solo di interesse giuridico, ma è anche d'interesse economico, perchè le condizioni giuridiche da tutelare incidono sul peso dei fattori produttivi e distributivi rispetto ai risultati, nonché sull'organizzazione del lavoro all'interno delle aziende.

L'art. 41 della Costituzione italiana afferma che l'iniziativa economica privata è "libera" e non deve svolgersi in contrasto con l'"utilità sociale" o

¹³⁶ Nel suo discorso di presentazione della Relazione sull'attività dell'Autorità Garante per la protezione dei dati personali relativa all'anno 2005, tenutosi in Roma il 7 luglio 2006, il Prof. FRANCESCO PIZZETTI ha osservato che “...La società della tecnica, già diventata nel secolo scorso una società “a cambiamento veloce”, è divenuta oggi una società “a cambiamento velocissimo”...” e che “...rispetto a questa incredibile metamorfosi, è naturale interrogarsi sulla possibilità dell'uomo di esercitare un ruolo di guida e di governo del progresso tecnico; sulla sua capacità di indirizzare l'uso della tecnologia, che è un mezzo, verso fini e risultati al servizio dell'uomo e rispettosi della sua dignità. La tecnologia può essere un formidabile strumento di libertà oppure causa di inedite differenziazioni sociali. È qui che si colloca il valore fondamentale racchiuso nelle regole e nei comportamenti in cui consiste il diritto alla privacy...”.

¹³⁷ GAETANO RASI, *Cosa cambia nelle attività produttive*, in *Da costo a risorsa. La tutela dei dati personali nelle attività produttive*, a cura di GAETANO RASI, Roma, 2004.

recando danno alla libertà e alla dignità umana¹³⁸.

Ciò nonostante, il trattamento dei dati personali nel rispetto della normativa vigente, che pure deve essere svolto nel rispetto dei diritti e delle libertà fondamentali, è generalmente avvertita dal mondo delle attività produttive come un vincolo e un freno.

È probabile che questa opinione trovi giustificazione nella strumentazione giuridica, che in alcuni casi è generale ed uniforme e, quindi, non coglie a pieno le differenze fra le diverse realtà produttive e le diseguali dimensioni di impresa.

In effetti, il Codice per la protezione dei dati personali di cui al Decreto Legislativo n. 196 del 30 giugno 2003, prevede diversi adempimenti per le imprese, pesantemente sanzionati ed obbliga le aziende ad investimenti di varia natura al fine di conformare i processi aziendali alla normativa rilevante in materia.

Occorre, pertanto, interrogarsi se un corretto trattamento dei dati personali debba intendersi in via esclusiva come un costo per le imprese, oppure possa risolversi in un utile investimento per le stesse, ovvero possa intendersi come una risorsa ed un valore aggiunto per le aziende.

2. Il diritto alla tutela dei dati personali e l'attività d'impresa.

Con riferimento all'attività d'impresa, la *Data Protection* assume rilievo, in particolare, rispetto al rapporto con i lavoratori, alla concorrenza ed alle relazioni con altri *partners* commerciali ed infine, rispetto al rapporto con i consumatori, ovvero i propri clienti, attuali e potenziali.

2.1. La tutela dei dati personali nel rapporto di lavoro.

Quello del rapporto di lavoro è uno degli ambiti in cui l'esigenza di tutelare il diritto alla riservatezza assume maggiore rilievo, in parte perchè tale diritto viene a porsi in contrasto dialettico con i diritti ed i poteri propri del datore di lavoro e, in parte, perché i due principali protagonisti di questo rapporto, datore e prestatore di lavoro subordinato, non si trovano mai su di un piano di eguale forza contrattuale ed economica, ciò che rischia in molti casi di tradursi in una disparità anche giuridica¹³⁹.

Peraltro, il già difficile compito di trovare un punto di mediazione fra questi interessi contrapposti, è reso anche più arduo dall'evolversi della tecnologia e dai diversi modi in cui nel tempo cambiano le forme organizzative dell'impresa.

¹³⁸ Non è stata enucleata una nozione generale e unitaria dell'espressione "utilità sociale". Trattasi di un concetto indeterminato e in costante evoluzione, da adattare ai tempi. Una cosa tuttavia è chiara: dietro le espressioni "utilità sociale" e "dignità umana" vi sono non tanto singoli beni individuali dell'uomo, quanto i valori costitutivi della soggettività umana e della personalità dell'individuo.

¹³⁹ GIOACCHINO QUADRI DI CARDANO, *Il trattamento dei dati nel rapporto di lavoro*, in *Il Codice in materia di protezione dei personali. Commentario sistematico al D.Lgs. 30 giugno 2003, n. 196*, a cura di JURI MONDUCCI e GIOVANNI SARTOR, Padova, 2004.

Ben si comprende, pertanto, la ragione della grande attenzione dedicata alla tutela della riservatezza dalla Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), che, pur non avendo ancora come punto di riferimento il dato personale, anticipa le finalità di tutela dell'uomo e dei suoi diritti nel loro complesso che sono state proprie della Legge 31 dicembre 1996, n. 675 e che ora vengono riprese dal nuovo Codice, in applicazione della Direttiva 95/46/CE.

Tuttavia il cambio di prospettiva dalla tutela della riservatezza a quella dei dati personali è estremamente significativo¹⁴⁰, non solo perché i dati dei lavoratori sono oggetto di un costante flusso – che in molti casi inizia già dalle fasi precedenti la stipulazione del contratto di lavoro – che deve essere in qualche modo governato, ma anche perché consente di liberarsi da ambigue e discutibili interpretazioni del concetto di “privatezza” o “vita privata”, con cui si è passato in cercato di limitare alcuni importanti diritti del lavoratore¹⁴¹. È evidente che il lavoratore, in forza del rapporto contrattuale che lo lega con il datore di lavoro, debba accettare un certo grado di intrusione nella propria sfera privata da parte di questo ultimo e condividere con esso alcuni dati personali.

Il datore di lavoro ha infatti un legittimo interesse a trattare alcuni dati personali relativi ai propri dipendenti per finalità legali e legittime, necessarie allo sviluppo normale del rapporto di lavoro ed al buon funzionamento dell'impresa.

La questione non è quindi determinare se il trattamento dei dati personali nel contesto lavorativo sia in sé lecito oppure no, bensì accertare i limiti che la protezione dei dati personali impone a questo tipo di attività e le

¹⁴⁰ Il Codice di cui al D.Lgs. 30 giugno 2003, n. 196, introduce nell'ordinamento il diritto alla protezione dei dati personali, quale diritto fondamentale della persona, che è parallelo e si integra col più generale diritto alla riservatezza. In tal modo il legislatore italiano si adegua al quadro normativo comunitario che nella Carta dei diritti fondamentali dell'Unione Europea, ha segnato una dualità di diritti (peraltro tra loro connessi) comprendendo nel Capo II della "Libertà" sia l'art. 7 "*Rispetto della vita privata e della vita familiare*": "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*"; sia l'art. 8 "*Protezione dei dati di carattere personale*": "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*". È stato esattamente osservato che l'art. 7 riguarda il momento individualistico della riservatezza e l'art. 8, invece, la protezione dei dati personali nei vari circuiti sociali, economici, culturali. Sicché la prima è una tutela statica; l'altra è una tutela dinamica. Cfr. GIUSEPPE CASSANO e STEFANO FADDA, in *Codice in materia di protezione dei dati personali: ratio esegetica e questioni sottese*, in *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy D.lgs. 30 giugno 2003, n. 196*, a cura di GIUSEPPE CASSANO e STEFANO FADDA, Milano, 2004.

¹⁴¹ Sul punto, nel caso *Niemits vs. Germania*, riguardante la perquisizione dell'ufficio del ricorrente effettuata da un'autorità governativa tedesca, la Corte Europea dei Diritti Umani, ha rigettato la tesi del governo tedesco secondo cui l'art. 8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali, opererebbe una netta distinzione tra vita privata e mura domestiche da un lato, e vita professionale e locali destinati all'attività professionale dall'altro, dichiarando che non vi è alcuna ragione di principio che consenta d'interpretare il concetto di vita privata nel senso di escludere attività di natura professionale e commerciale, perché è nel corso della propria lavorativa che la maggior parte delle persone ha la possibilità di sviluppare relazioni con il mondo esterno.

ragioni che possono giustificare la raccolta ed il trattamento dei dati personali di un determinato lavoratore.

Per fare ciò è necessario tenere conto non solo della legislazione specifica in materia di *privacy*, ma anche della normativa posta a tutela del lavoratore¹⁴² ed, in particolare, dello Statuto dei Lavoratori, il cui ambito di applicazione non è stato certo ridotto dalla Legge 31 dicembre 1996, n. 675, prima e dal Codice per la protezione dei dati personali, poi e le cui disposizioni hanno in molti casi funzione integrativa e non sostitutiva, operando alcuni significativi rinvii ai principi e precetti contenuti nello Statuto.

2.2. La tutela dei dati personali e la concorrenza.

Nel sistema economico, la tutela dei personali, assume interesse anche con riferimento alla concorrenza ed al libero mercato.

Difatti, il diritto alla tutela dei dati personali è diritto di tutti, anche delle imprese e la circolazione delle informazioni può essere un fattore di crescita per la concorrenza, oppure prestarsi a condotte lesive della stessa.

Il diritto alla riservatezza, adeguandosi alle nuove esigenze di una società sempre più dinamica e capace di far circolare le informazioni con straordinaria velocità, si risolve nel diritto ad esercitare un controllo sui dati personali, ovvero nel diritto di stabilire, se, come e quando le informazioni che ci riguardano possono essere raccolte e messe a disposizione degli altri.

L'art. 1 del Codice per la protezione dei dati personali riconosce il diritto di "chiunque" alla protezione dei dati personali, quale autonomo diritto rispetto al diritto alla riservatezza, esercitabile da qualsiasi figura soggettiva in relazione al trattamento dei propri dati personali.

Cosicché, la legge italiana, a differenza di quanto prevedono le analoghe discipline straniere e la direttiva comunitaria per la tutela dei dati personali, prevede che possano essere tutelati anche i dati che riguardano le persone giuridiche¹⁴³.

L'immediata conseguenza è che, in linea teorica, un'impresa che ritenesse di aver subito un trattamento non autorizzato dei propri dati personali,

¹⁴² Cfr. Legge 29 febbraio 1980 n. 33, art. 2, che, nel disciplinare le modalità di comunicazione del certificato di malattia, da parte del lavoratore, sia al datore di lavoro che all'ente previdenziale cui compete il pagamento dell'indennità di malattia, prevede che il certificato da inviare all'ente previdenziale sia completo sia della diagnosi della patologia sofferta dal lavoratore che della prognosi, prevede che solo quest'ultima sia indicata nei giustificativi di assenza per malattia destinata al datore di lavoro. E ancora, l'art. 6 della Legge 5 giugno 1990, n. 135 proibisce in maniere assoluta ai datori di lavoro, pubblici e privati, lo svolgimento di indagini volte ad accertare nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro l'esistenza di uno stato di serietà disponendo – in caso di violazione – l'applicazione del sistema sanzionatorio previsto dall'art. 38 dello Statuto dei Lavoratori.

¹⁴³ Il Codice - come la Legge n. 675/96 - si differenzia dalla direttiva europea 95/46/CE cui si ispira, la quale, ai sensi dell'art. 1, prevede che "gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali", escludendo quindi dall'ambito della sua operatività le informazioni relative alle persone giuridiche, enti e associazioni.

o comunque una fuga di notizie relative alla sua organizzazione interna, potrebbe legittimamente rivolgersi ai suoi concorrenti per esercitare i diritti di cui all'art. 7 e ss. del Codice per la protezione dei dati personali.

In caso di mancata risposta o di risposta inadeguata, l'impresa potrebbe chiedere l'intervento del Garante o adire l'autorità giudiziaria.

Quindi, ampie e diversificate forme di tutela si offrirebbero al soggetto che ha subito un trattamento non autorizzato di dati personali, senza considerare che proprio l'esercizio del diritto alla tutela dei dati personali, si propone come strumento indiretto di tutela rispetto all'illecita attività di spionaggio industriale¹⁴⁴.

Circa i rapporti tra la tutela dei dati personali e la concorrenza, ulteriore profilo d'interesse si ravvisa nella potenzialità della *privacy* di prestarsi a condotte collusive tra le imprese¹⁴⁵.

Se la concorrenza perfetta implica come condizione necessaria una puntuale e completa informazione tra tutti gli operatori, ovvero l'assenza di asimmetrie informative, è anche vero che lo scambio di tali informazioni può trasformarsi in uno strumento che facilita condotte collusive.

Il punto è chiarire sino a che punto sia consentito lo scambio di informazioni tra imprese, perché utile a rendere il mercato trasparente e ad incentivare strategie competitive a vantaggio del consumatore, posto che detto scambio consente comunque un coordinamento, implicito o esplicito, tra imprese concorrenti.

Perché uno scambio d'informazioni tra imprese concorrenti possa valutarsi lecito o meno, è necessario esaminare diversi fattori e, *in primis*, la natura dei dati trattati.

Per cui, lo scambio di dati sensibili tra imprese quali segreti aziendali, informazioni sulle strategie d'impresa (prezzi o politiche di *marketing*) o sulla struttura dell'impresa (costi o funzione di domanda), è elemento potenzialmente sufficiente per individuare uno spirito anticoncorrenziale della condotta.

Altri elementi da considerare sono la modalità ed i tempi e con i quali si realizza lo scambio di informazione tra le imprese.

Potenzialmente lesivo della concorrenza e indice di una condotta collusiva tra imprese, è lo scambio di informazioni in modo disaggregato, ovvero in una forma tale da consentire all'impresa concorrente di risalire alle informazioni sui singoli operatori.

E ancora, uno scambio di informazioni tra imprese concorrenti in modo sistematico e ravvicinato nel tempo consente un grado di conoscenza e una capacità di reazione tale da agevolare il reciproco coordinamento su equilibri concorrenziali.

Altro elemento è la divulgazione limitata ai partecipanti allo scambio di

¹⁴⁴ MARCO MAGLIO, *Privacy e concorrenza sleale: e ora mi dirai cosa hai spiato? L'autodisciplina tra le regole di mercato e lo specchio di Narciso*, in *Interlex*, 15 ottobre 1997.

¹⁴⁵ GIUSEPPE TESAURO, *Competizione economica: i vantaggi della protezione dei dati*, in *Da costo a risorsa. La tutela dei dati personali nelle attività produttive*, a cura di GAETANO RASI, Roma, 2004.

tali informazioni. Si tratta forse del fattore centrale nell'analisi, dal momento che se i dati vengono utilizzati solo tra gli operatori concorrenti, la loro funzione non può che essere quella di strumento facilitante la collusione, essendo veicolo per l'osservazione delle azioni e pertanto reazione tra le imprese.

Viceversa, se le osservazioni sono rese pubbliche, ovvero sono divulgate ai consumatori, è possibile che queste assumano la veste di strumento che aumenta la trasparenza del mercato, facilita il confronto tra i prezzi, la qualità e la gamma dei prodotti e quindi incentiva il gioco competitivo tra le imprese.

Non è facile distinguere se e quando i dati oggetto di scambio meritano protezione, ovvero devono necessariamente rimanere nell'ambito dell'impresa e non diventare oggetto di scambio tra concorrenti, o viceversa meritato la medesima divulgazione per favorire il confronto concorrenziale.

È tuttavia evidente che un'informazione chiara e trasparente al pubblico dei consumatori, in grado di rendere agevole la valutazione delle tariffe, il confronto e la comparazione sui parametri tra imprese, potrebbe essere uno strumento importante per rendere trasparente il mercato, aumentare il grado di conoscenza del consumatore sul servizio e quindi indurlo a porre in concorrenza le imprese nella formulazione sulle offerte.

2.3. La tutela dei dati personali ed il rapporto con i consumatori e gli utenti. L'attività di *marketing* e lo *spamming*.

Il progresso tecnologico e, in modo particolare, la rivoluzione informatica e telematica sulla quale si fonda la Società dell'Informazione, ha comportato profondi e radicali cambiamenti nelle dinamiche del commercio e del mondo imprenditoriale, fornendo agli operatori strumenti di *business* e metodi commerciali e di *marketing* nuovi¹⁴⁶.

Uno degli effetti più rilevanti di questa autentica rivoluzione culturale, prima ancora che economica e commerciale, è certamente rappresentato dai profondi mutamenti che si sono prodotti sul versante del rapporto tra il mondo imprenditoriale e quello degli utenti e consumatori.

Un tempo l'impresa si rivolgeva in modo indiscriminato ai propri potenziali clienti a prescindere dall'acquisizione di qualsivoglia genere d'informazione circa la loro propensione all'acquisto, l'appartenenza a questa o a quella classe sociale, reddituale o culturale. Detto contesto, oggi, è radicalmente mutato.

La principale differenza tra le relazioni di mercato di ieri e quelle attuali, sta nel mutato approccio delle aziende verso la propria potenziale clientela.

Il consumatore, un tempo, non era preso in considerazione in quanto

¹⁴⁶ GUIDO SCORZA, *Il Marketing*, in *Il codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003, n. 196*, a cura di JURI MONDUCCI e GIOVANNI SARTOR, Padova, 2004.

individuo, ma come un membro di un gruppo omogeneo, privo di diversificazione, mentre oggi, proprio grazie ai moderni mezzi di comunicazione telematica ed interattiva, tendono ad affermarsi nuovi metodi fondati sulla personalizzazione dei messaggi pubblicitari.

Il consumatore si trova al centro di una rete di messaggi che convergono per indurlo all'acquisto, facendo leva sui suoi specifici interessi e bisogni individuali. Ciò ha determinato il passaggio dal mercato rivolte alle masse, al mercato rivolto all'individuo.

Ma non sono solo i momenti del "contatto commerciale" e dell'"invito all'acquisto" ad essere mutati. Anche la fase post – vendita e, quindi, i servizi offerti a chi è già diventato cliente, risente fortemente della possibilità tecnica di modulare l'assistenza, assecondando le mutevoli e diversificate esigenze del consumatore.

Non a caso da tempo, ormai, le aziende parlano di fidelizzazione del cliente e investono ingenti risorse per gestire con attenzione il rapporto con il cliente e per prostrarlo nel corso del tempo.

In altre parole, se nella visione classica del *marketing*, l'obiettivo cui dovrebbe tendere l'impresa è la soddisfazione del cliente, senza la necessità di alcun investimento tecnico o organizzativo per cercare di sviluppare la relazione, nel "*marketing relazionale*", la soddisfazione del cliente è solo il punto di partenza che, combinato con altre elementi, conduce alla fedeltà del cliente.

Seguendo tale impostazione nasce il concetto di *Customer Relationship Management* (CRM), ossia un modello di gestione capace di generare, mantenere e sviluppare le relazioni con i clienti.

Appare pacifico che detto mutato contesto sia determinato prevalentemente dallo sviluppo di tecnologie di trattamento e di analisi delle informazioni sui consumatori, che favoriscono l'adozione di politiche di *marketing* più efficaci in quanto in grado di evitare la dispersione dell'offerta verso obiettivi errati.

Da ciò discende, dunque, in modo altrettanto lineare, l'esigenza d'individuare, in modo puntuale ed urgente, un quadro normativo primario e secondario che stabilisca, in modo chiaro ed univoco, limiti e garanzie per la realizzazione di tali specifiche forme di trattamento di dati personali.

In questa prospettiva, ai sensi dell'art. 140 del Codice per la protezione dei dati personali, "*Il Garante promuove, ai sensi dell'art. 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato ai fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni*".

Le attività di *direct marketing* appaiono, dunque, suscettibili di sollevare, con riferimento alla disciplina in materia di tutela dei dati personali,

due distinte problematiche giuridiche.

La prima è connessa alla violazione della sfera personale dell'individuo, che può realizzarsi ogni qual volta questi riceva una comunicazione commerciale non sollecitata.

Si tratta di una questione avente origini ormai risalenti nel tempo ma che sta conoscendo una fase di ritrovata vitalità per l'effetto del progressivo diffondersi della posta elettronica che, indubbiamente, costituisce uno strumento particolarmente congeniale a tale genere di pratica commerciale nota con le espressioni anglosassoni di *spamming*, ovvero con l'acronimo UCE – *Unsolicited Commercial E.Mail*¹⁴⁷.

La seconda problematica concerne invece i rischi connessi alle attività di profilazione degli utenti e dei consumatori quotidianamente svolte in ambiente telematico o, comunque, attraverso le nuove risorse informatiche e telematiche, in quanto prodromiche alla realizzazione delle campagne di *direct marketing*¹⁴⁸.

Sul terreno del *marketing* nella Società dell'Informazione si confrontano, dunque, interessi contrapposti ed egualmente meritevoli di tutela. Se, da un lato, non può, infatti, dubitarsi del carattere irrinunciabile del diritto alla protezione dei propri dati personali, dall'altro occorre, comunque, riconoscere che il rilievo di tale diritto non può giustificare un'integrale compressione di quelli connessi al libero esercizio di un'attività imprenditoriale, diritti, questi ultimi, che trovano un loro preciso fondamento, per un verso, nell'art. 41 della Costituzione Italiana e, per l'altro verso, nella Direttiva 2000/31/CE dell'8 giugno 2000 "*Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno (Direttiva sul commercio elettronico)*", laddove, al considerando 29, è stato espressamente dato atto che "*le comunicazioni commerciali sono essenziali per il finanziamento dei servizi della società dell'informazione e per lo sviluppo di un'ampia gamma di nuovi servizi gratuiti*".

¹⁴⁷ Sul punto, l'art. 130 del Codice per la protezione dei dati personali, rubricato "*Comunicazioni indesiderate*" e che affianca l'art. 140 *cit.* in materia di *Marketing Diretto*, disciplina il fenomeno dello *spamming* e non solo, fornendo regole applicabili a tutte le forme di promozione e commercializzazione diretta effettuate sfruttando le potenzialità offerte dalle tecnologie informatiche e telematiche, che consentono, con un impegno di risorse umane ed economiche molto limitato, di raggiungere un numero elevatissimo di soggetti ampliando a dismisura l'effetto di queste strategie commerciali. È proprio il rapporto tra i costi necessari a predisporre la struttura per effettuare questo tipo di attività ed i vantaggi conseguibili in termini di numero di utenti potenzialmente raggiungibili che ha determinato il successo di queste forme di commercializzazione, provocando la reazione dell'opinione pubblica e del legislatore, per porre fine ad un fenomeno che determina forti interferenze nella vita privata degli utenti.

¹⁴⁸ VITTORIO FROSINI, in *La carta d'identità informatica: il profilo perfetto di una persona*, in *Telega*, 20, 2000, ritiene che "...si è dunque infine aperta la prospettiva della creazione di un'identità informatica costruita con diversi attributi particolari di carattere sociale, riuniti in un profilo unitario che consente una configurazione dell'individuo sempre più precisa...l'immagine virtuale diverrà sempre più nitida, si sovrapporrà a quella reale nel controllo esercitato dall'autorità pubblica sulla privata dell'individuo...".

3. I costi della tutela dei dati personali.

Diffusa è la discussione in merito al “costo *privacy*” ed ai criteri di valutazione economica del trattamento dei dati personali.

In realtà, è difficile valutare quale sia e a quanto ammonti il “costo *privacy*”, perché la tutela dei dati personali ha, quale presupposto, il potere di scelta riservato all’individuo circa l’ambito da riservare alla circolazione dei propri dati personali.

La definizione del livello di *privacy*, nasce essenzialmente da una scelta individuale, per cui occorre chiedersi secondo quali criteri dette scelte vengono effettuate e quali conseguenze producono queste scelte individuali rispetto al benessere complessivo della società.

L’obiettivo del *Data Protection* ha un forte impatto sui sistemi aziendali, in quanto richiede un processo di riorganizzazione degli stessi, nonché un adeguamento strutturale, in termini di infrastrutture tecnologiche, gestione dei processi organizzativi, formazione ed aggiornamento del personale.

Accanto a questo costo, che può essere direttamente misurabile all’interno dell’impresa, bisogna aggiungere la “spesa” misurata in termini sociali: data dalla proliferazioni di leggi e dalla scarsa efficienza e burocratizzazione del sistema con il quale si devono misurare tutte le aziende. Autorevole dottrina¹⁴⁹ ritiene che possano individuarsi diverse categorie di costi in relazione a tre specifici criteri: 1) i soggetti che sopportano tali costi; 2) il tempo in relazione al quale sono sostenuti tali costi; 3) gli effetti derivanti dai costi.

Dal punto di vista soggettivo è possibile parlare di costi individuali, ovvero i costi sostenuti tanto dall’interessato per esercitare i suoi diritti di riservatezza, quanto dal titolare per adeguarsi alla protezione dei dati personali, e di costi sociali, ovvero i costi che la collettività sopporta per garantire il rispetto della riservatezza individuale. In questo contesto rientrano i costi di organizzazione che lo Stato sostiene per rispondere alla domanda di *privacy* dei cittadini.

Dal punto di vista cronologico va osservato che i costi possono essere sostenuti in via preventiva, al fine di evitare che si verifichino violazioni della *privacy* oppure successivamente, per porre rimedio a violazioni della *privacy* che si siano già verificate.

Sono costi preventivi, i costi da sostenersi per l’inserimento e la formazione delle risorse umane da destinare alla gestione delle procedure in materia di *privacy*, per lo sviluppo e l’aggiornamento delle procedure interne in materia di *privacy*, per la verifica delle attività di gestione della *privacy*, per l’adozione di strumenti tecnologici ed informatici che garantiscano la protezione dei dati personali, per la comunicazione interna diretta a diffondere

¹⁴⁹ MARCO MAGLIO, *Analisi economica del diritto alla riservatezza*, in *Da costo a risorsa. La tutela dei dati personali nelle attività produttive*. A cura di GAETANO RASI, Roma, 2004.

le *privacy policies* e per gestire la relazione diretta con i soggetti cui si riferiscono i dati personali trattati.

Sono costi successivi, i costi da sostenersi per conformare i sistemi di gestione dei dati alla normativa rilevante in materia di protezione dei dati personali, nonché i costi connessi a sanzioni amministrative, risarcimento dei danni, lesione dell'immagine aziendale.

Con riferimento agli effetti, infine, i costi possono essere distinti in costi di transazione, ovvero, in termini economici, l'investimento legato alla scelta effettuata ed in costi di opportunità, ossia le rinunce che ogni soggetto è disposto a sostenere in conseguenza della propria scelta.

È con riferimento al criterio scelto, che è possibile valutare oggettivamente i costi ed individuare i rischi che un'organizzazione affronta rispetto al trattamento dei dati personali e l'indice di investimento che deve sostenere per ridurre adeguatamente questi rischi.

Finora, il confuso dibattito sui costi della *privacy*, si è sviluppato considerando, in via esclusiva, i costi di prevenzione e correttivi, nonché i costi di transazione, evidenziando solo l'impatto negativo nascente dall'esistenza di costi monetari.

Tuttavia, perché i costi della *privacy* possano essere correttamente apprezzati ed eventualmente valutati in termini di investimento aziendale, andrebbe valorizzata la riflessione sui costi opportunità, perché sono quelli che incidono più direttamente sul meccanismo di tutela dei dati personali.

Per costo opportunità, deve intendersi la rinuncia a una possibile alternativa. Esso è rappresentato dal valore che viene dato all'alternativa migliore alla quale si rinuncia adottando un certo comportamento.

L'interessato posto di fronte alla scelta di concedere o meno il consenso al trattamento dei dati personali, compie una valutazione dei costi opportunità derivanti da quella decisione, comparando i benefici nascenti dalle possibili alternative.

Se decide di limitare la circolazione dei suoi dati personali rinuncia all'opportunità di entrare in contatto con chi gli ha chiesto il consenso, ma in questo modo rafforza il proprio livello di riservatezza.

Al contrario, se sceglie di consentire il trattamento, riduce il livello di riservatezza dei propri dati, ma aumenta le possibilità di entrare in contatto con altri soggetti.

Allo stesso modo, il titolare di un trattamento che deve decidere se chiedere all'interessato il consenso per ulteriori iniziative rispetto ai suoi dati, fa una valutazione in termini di costi opportunità.

La mancata richiesta ridurrà i costi derivanti dalla gestione dei consensi, ma ridurrà anche l'opportunità di entrare nuovamente in contatto con l'interessato.

In termini economici, il meccanismo di funzionamento della *privacy* è condizionato dalla comparazione tra i costi opportunità dell'interessato e quelli del titolare del trattamento dei dati.

Se il vantaggio del titolare del trattamento derivante dal rispetto delle

norme in materia di trattamento dei dati personali, si somma a quello dell'interessato, si verifica un riequilibrio del sistema in cui il livello di *privacy* non dipende più solo dalla scelta dell'interessato, ma viene sollecitato dallo stesso titolare, cosicché la *privacy* assume un valore trasversale che porta benefici condivisi, che riguardano tanto il singolo che la collettività, tanto i cittadini quanto le imprese, ovvero, in altri termini, diventa una risorsa per l'azienda ed suo elemento competitivo.

4. La tutela dei dati personali come qualità e risorsa aziendale.

In un mondo in cui l'uso di dati è condizione vitale per la crescita economica e spesso per la sopravvivenza delle imprese, la protezione dei dati personali è una necessità.

Se il portafoglio ordini, i sistemi di approvvigionamento, i dati relativi ai dipendenti, ai consulenti, ai clienti, non sono protetti, può essere a rischio una parte essenziale del patrimonio aziendale, dell'avviamento commerciale, del valore stesso del marchio.

Non esiste attualmente un sistema di misurazione dell'influenza della qualità derivante dal corretto trattamento dei dati personali, nelle attività economiche e la mancanza di un sistema di valutazione dell'investimento *privacy* non consente di replicare, in termini concreti, al comune sentire per cui la normativa di settore costituirebbe un limite al libero esercizio dell'attività imprenditoriale, se non un ostacolo alla crescita economica¹⁵⁰.

Un corretto trattamento dei dati personali appare, tuttavia, rilevante in relazione all'importanza che le imprese attribuiscono alle informazioni sui propri dipendenti e collaboratori, sui propri clienti attuali e potenziali, sulla moralità e puntualità nei pagamenti da parte dei propri *partners* commerciali.

Dall'altro, è di pari rilievo l'attenzione che i dipendenti ed i consumatori riservano alle *privacy policies* adottate da parte delle imprese.

Il rispetto della normativa rilevante in materia di trattamento dei dati personali quale valore aggiunto ed elemento competitivo per le imprese, è stato esaminato, in particolare, proprio con riferimento al rapporto tra imprese e consumatori¹⁵¹.

È interesse delle imprese verificare in che termini, il corretto trattamento dei dati personali del consumatore, possa incidere sul processo di

¹⁵⁰ Secondo una ricerca di ROLAND BEGER che si occupa in specifico delle aree del *Direct Marketing* e del *Telemarketing* compresi i servizi effettuati dai contact center e l'impatto sulle vendite a distanza, presentata nel luglio 2005 alla stampa dal Comitato Interassociativo del Marketing Diretto che riunisce la maggior parte delle associazioni italiane del settore (Assocontact, Assografici, Assomed, Assocomunicazione e Unicom), il corretto trattamento dei dati personali, porterebbe con sé effetti collaterali indesiderati: occupazione a rischio, sviluppo economico compromesso, difficoltà di comunicazione diretta tra imprese e consumatori, barriere all'entrata di nuovi operatori, impatto negativo sulla libera concorrenza e sui prezzi.

¹⁵¹ DAVID BERGANTIN e ROBERTO GALBIATI, *Il rispetto della privacy risorsa chiave del CRM. L'adozione di comportamenti etici è in grado di differenziare le aziende che agiscono senza il rispetto per la privacy da quelle che rispettano tale condizione*. Relazione tenuta in occasione della Conferenza Internazionale svoltasi a Roma, il 5-6 dicembre 2002, *Privacy: da costo a risorsa*.

consolidamento della relazione di fiducia con il consumatore e, da un punto di vista etico, quali comportamenti adottare nei confronti del consumatore per non minare la propria capacità relazionale.

I livelli di *privacy* d'interesse del consumatore sono diversi e riguardano il tipo di informazioni raccolte dalle imprese, le modalità di raccolta delle stesse, la figura del titolare dei trattamenti dei dati e degli eventuali responsabili ed incaricati dei trattamenti, le conseguenze ed i benefici offerti nello scambio d'informazioni di natura personale.

Le imprese devono dichiarare apertamente la tipologia dei dati trattati, le modalità e le finalità di detti trattamenti: ignorando questo aspetto, esse corrono il rischio di attivare un processo di profonda sfiducia da parte del consumatore.

Il livello di tutela dei propri dati personali che il consumatore chiede all'impresa e che l'impresa garantisce al consumatore, favorisce la volontà del consumatore di relazionarsi all'impresa e lo sviluppo di una relazione di fiducia con la stessa.

L'assenza o l'insufficienza di una politica aziendale in materia di tutela dei dati personali, crea sfiducia nel consumatore, incide negativamente sulla sua volontà relazionale e porta con sé il rischio, grave per l'impresa, che il consumatore non fornisca informazioni personali o fornisca informazioni incomplete o false.

È sul piano dell'acquisizione, dell'elaborazione e della gestione dei dati del consumatore, inoltre, che l'impresa può adottare una serie di comportamenti "etici" capaci di aumentare la fedeltà del consumatore.

L'adozione di comportamenti etici è in grado di differenziare le imprese che agiscono senza il rispetto per la *privacy*, da quelle che rispettano tale condizione. Parlare di etica "relazionale", quindi, significa impiegare le politiche e le strategie aziendali per ridurre le incertezze dei clienti riguardo al problema della *privacy* e aumentarne il grado di fiducia e di fedeltà verso l'azienda.

I consumatori, infatti, saranno meno ansiosi del potenziale abuso o delle conseguenze negative risultanti dalla raccolta delle loro informazioni, se vi è un senso di fiducia verso l'organizzazione ed una condivisione delle politiche di *marketing*.

Conclusioni.

La tutela dei dati personali, a fronte della sua onerosità, favorisce un complesso processo di inventario e di riordino dell'intero patrimonio informativo dell'azienda.

Il "costo *privacy*" consente, pertanto, di evitare situazioni negative che potrebbero divenire anche critiche per l'azienda quali: la riduzione delle vendite; la sfiducia da parte dei clienti; l'immagine negativa; i contenziosi giudiziari.

Al contrario, mediante il rispetto dei principi etici, di correttezza e

trasparenza, sono certi una serie di vantaggi quali: un migliore rapporto fiduciario con gli interessati; una buona immagine globale; processi decisionali percepiti come rispettosi dei lavoratori e dei clienti e, in genere, dei soggetti esterni (anche concorrenti e fornitori); prevenzione dei contenziosi giudiziari. La ricerca dell'equilibrio nel sistema di protezione dei dati personali è essenziale per rendere possibile uno sviluppo effettivo.

La cultura della riservatezza nel nostro Paese sta sempre più diffondendosi¹⁵² e la tutela dei dati personali sta diventando un'esigenza propria del mercato, per cui le imprese che non risponderanno a questo nuovo tipo di domanda rischieranno di uscire dal mercato.

Si delinea, in definitiva, un nuovo modello di competitività, in relazione al quale l'offerta dei prodotti e dei servizi che non corrisponde alla richiesta di rispetto della tutela dei dati personali, incontrerà sempre maggiori difficoltà a trovare e mantenere fedeli gli acquirenti.

È necessario che il mondo imprenditoriale comprenda che il rispetto del diritto alla *privacy* non rappresenta solo ed esclusivamente una voce di costo nel bilancio delle aziende. Se efficacemente utilizzato, può costituire un valore aggiunto per l'impresa ed un elemento di fidelizzazione del consumatore verso i prodotti ed i servizi commercializzati da soggetti più rispettosi dei propri interessi in termini di riservatezza e, per questa via, un importante elemento concorrenziale.

Ebbene, dopo anni di tentativi effettuati dall'Autorità Garante per la protezione dei dati personali, diretti a sensibilizzare le aziende sull'importanza della tutela della *privacy* e di interventi di regolamentazione in diversi settori, frutto di un'attività di concertazione con i soggetti interessati¹⁵³, le aziende sembrano finalmente aver preso coscienza autonomamente della necessità di assicurare il giusto grado di protezione ai dati personali di cui sono titolari.

¹⁵² Scheda di documentazione ed analisi sintetica, Fonte: Eurobarometro 2003, Speciale Data Retention, Realizzata da ANNA CAROLA FRESCHI. CAMBIO – Il Laboratorio di ricerca sulle trasformazioni sociali – Università di Firenze, Polo delle Scienze Sociali. Scheda presentata in occasione del Convegno *E.Privacy 2004*, tenutosi a Firenze il 14 - 15 maggio 2004.

¹⁵³ Nel suo discorso di presentazione della Relazione sull'attività dell'Autorità Garante per la protezione dei dati personali relativa all'anno 2005, tenutosi in Roma il 7 luglio 2006, il Prof. FRANCESCO PIZZETTI ha sintetizzato l'attività svolta dell'Autorità Garante con riferimento al sistema economico per cui "...abbiamo monitorato l'attuazione del codice deontologico nel settore del credito al consumo; un settore che, nel 2005, ha movimentato una cifra pari a 76 miliardi di euro. Abbiamo regolato le attività di marketing e di profilazione nella grande distribuzione commerciale e nell'offerta di servizi di vario genere, vietando quelle svolte senza il consenso dei consumatori. È in questo quadro che si collocano il provvedimento generale sulle cd. "carte di fedeltà", che sono oltre 30 milioni, e un recente provvedimento che ha vietato trattamenti illeciti nel settore alberghiero. Abbiamo prestato la consueta attenzione alla tematica relativa alla tutela delle informazioni personali dei lavoratori, che presenta sempre nuove dimensioni e sfaccettature: ricordiamo, in particolare, l'utilizzo del sistema RFID che può determinare forme gravemente pervasive di controllo sulla vita del lavoratore. Con riferimento alle relazioni tra cittadini e attività economiche, segnaliamo i provvedimenti sulle società di recupero crediti; sui rapporti dei cittadini con le compagnie assicurative; sulle corrette modalità di uso del telepass; sul rapporto tra utenti e servizi di radio-taxi. Massima cura abbiamo dedicato ad agevolare l'aggiornamento della normativa antiriciclaggio. Tenendo presente la necessità di garantire la libertà di commercio e di circolazione dei beni, abbiamo rilasciato nuove autorizzazioni generali e dato esecuzione alle decisioni della Commissione europea sul trasferimento dati verso Paesi terzi, in applicazione dell'istituto delle clausole contrattuali tipo...".

L'indagine *Global Information Security Survey* pubblicata di recente da *Ernst & Young*, ha identificato che la tematica della protezione dei dati personali e della *privacy*, si è posta oggi all'attenzione del *management* aziendale, perché fattore prioritario per il successo dell'attività d'impresa.

Lo studio riporta il punto di vista di circa 1200 *managers* della sicurezza informatica operanti in 48 paesi. Per quanto riguarda l'Italia, il campione nazionale concorda nell'individuare la *privacy* come uno dei principali fattori nello sviluppo di strategie di sicurezza informatica: il 93% degli intervistati ha dichiarato, infatti, che questo è stato il tema che, negli ultimi 12 mesi, ha maggiormente coinvolto la funzione *Information Security* nella propria organizzazione.

Le aziende hanno preso coscienza del fatto che la problematica relativa alla tutela della *privacy* e dei dati personali è molto vasta, per cui l'esigenza continuerà ad essere prioritaria e richiederà particolare attenzione nella definizione delle misure atte a prevenire i rischi. Anche nei prossimi 12 mesi, infatti, per il 67% degli interpellati italiani, questo tema continuerà ad essere prioritario e ad attirare significativi investimenti.

E ancora, la conformità alle norme ed ai regolamenti di settore, si dimostra il principale obiettivo che guida le attività di *Information Security*. Circa l'80% dei partecipanti allo studio è infatti concorde nel sostenere che gli impegni e le attività indirizzate al raggiungimento della conformità a norme e regolamenti, hanno significativamente contribuito al miglioramento della *Information Security* aziendale.

Contestualmente al riconoscimento dell'importanza della protezione dei dati personali, le aziende hanno mostrato un'accresciuta sensibilità circa le azioni richieste per gestire i rischi connessi al trattamento dei dati personali da parte di soggetti terzi, specialmente in merito all'utilizzo dei dati aziendali da parte di fornitori di servizi in *outsourcing*.

Il *management* aziendale, dunque, una volta implementato un piano di protezione per i dati personali, non vuole vanificare gli sforzi affidandoli a terze parti che non ne garantiscono lo stesso livello di sicurezza.

I rapporti con i *partners* vengono inclusi nel piano generale di protezione dei dati, vengono stabiliti *standards* di sicurezza che regolano i rapporti con i terzi, dando origine, dunque, ad un circolo "virtuoso" di cui beneficia il sistema economico nel suo complesso.

E' indubbio che con il Codice per la protezione dei dati personali, il Garante abbia fornito chiari segnali di non voler più transigere, pretendendo il rispetto di quanto contenuto nella normativa.

Tuttavia, in un'ottica di *business*, gli investimenti effettuati devono essere seguiti da un maggior ritorno economico, per cui, solo nel momento in cui le nuove minacce informatiche hanno dimostrato di puntare allo sfruttamento dei dati personali e al furto delle identità, con il rischio di generare gravi perdite economiche per le aziende, queste hanno finalmente scoperto l'importanza di proteggere i dati sensibili.

Se a questa consapevolezza da parte delle aziende, si affiancassero

interventi positivi dell'Autorità Garante diretti a diffondere la cultura della riservatezza nel nostro Paese - per cui non solo un rigido sistema sanzionatorio - e forme di sgravio fiscale per gli investimenti aziendali in sicurezza e per l'adeguamento alla normativa di settore, così come richiesto dal mondo delle imprese, si assisterebbe, probabilmente, ad una reale attuazione della normativa in materia di tutela dei dati personali.

CAPITOLO VII

LAURA PEA

L'ANALISI DEI RISCHI NEL D.P.S. DEGLI ENTI LOCALI: LE RESPONSABILITÀ ASCRIVIBILI AL DIPENDENTE

SOMMARIO: 1. Premessa. – 2. La normativa in materia di sicurezza informatica. – 3. Il concetto di sicurezza. – 4. La normativa in materia di sicurezza informatica. – 5. La sicurezza informatica negli anni '90. – 6. Il boom di internet. – 7. La sicurezza informatica negli anni 2000. – 8. I dati dell'Osservatorio sulla sicurezza e Criminalità ICT (OCI). – 9. Il trattamento dei dati. – 10. Lo standard ISO/IEC17799:2000. – 11. Il trattamento dei dati negli EE.LL. – 12. L'analisi dei rischi. – 13. I Comportamenti degli operatori. – 14. Gli Insider. – 15. Eventi relativi agli strumenti. – 16. Eventi relativi al contesto. – 17. Le responsabilità del dipendente. – 18. Pronunce giurisprudenziali. – 19. Conclusioni.

1. Premessa

Scopo del presente scritto è la sensibilizzazione delle problematiche di sicurezza informatica relativamente al trattamento dei dati personali nell'ambito delle pubbliche amministrazioni, con particolare riferimento a quelle locali.

Partendo dalla definizione del concetto di sicurezza, è stata realizzata un'analisi cronologica dei rischi informatici, dall'inizio dell'era di Internet ai nostri giorni, dalla quale è emersa un'evoluzione delle tecniche di sabotaggio ed attacco nell'ambito del pubblico impiego.

A seguito di tale ricerca, sono stati analizzati più in dettaglio i rischi connessi al trattamento dei dati con strumenti informatici, sia da parte di comportamenti degli operatori, sia a causa di eventi relativi agli strumenti, che a causa di eventi relativi al contesto.

Relativamente ai rischi connessi ai comportamenti degli operatori, si è esaminato l'ambito tra le responsabilità ascrivibili al dipendente e quelle relative all'adozione delle misure di sicurezza aziendali.

Particolare accento è stato dato all'emergente rischio degli attacchi informatici provocati dagli insider, personale dipendente che - per vari motivi - è in grado di danneggiare o alterare il patrimonio informativo aziendale sfruttando la propria conoscenza della struttura interna del sistema informativo.

Infine sono state esposte alcune pronunce giurisprudenziali relative alle responsabilità riconosciute a dipendenti in merito al trattamento dei dati e degli strumenti informatici.

2. La normativa in materia di sicurezza informatica

Come già evidenziato in altri contesti, la normativa inerente la

sicurezza informatica - in ambito sia privato che pubblico - presenta un aspetto non unitario dovuto alla frammentaria e occasionale attenzione prestata all'argomento, conseguente alla carenza di un preciso e dettagliato indirizzo politico ed amministrativo almeno fino all'anno 2001. Un primo accenno di sensibilizzazione rispetto al problema può essere riscontrato nella Circolare della Funzione Pubblica n° 51223 del 21.05.1990, circolare che riportava un paragrafo dedicato ai criteri generali per la sicurezza fisica delle installazioni e per la sicurezza logica delle applicazioni. Successivamente il D.Lgs n° 39/1993 (che contestualmente istituisce l'AIPA - oggi CNIPA) ha dettato i criteri tecnici riguardanti la sicurezza dei sistemi. Negli anni a seguire si è quindi assistito ad un proliferare di atti, circolari, decreti in materia di sicurezza informatica che hanno investito vari aspetti tecnologici: la firma digitale, la posta elettronica, la RUPA, la Carta di Identità Elettronica, il protocollo informatico, ecc. fino ad arrivare al "recente" Decreto Legislativo 196 del 30.06.2003 (di seguito Codice) in materia di protezione del trattamento dei dati personali, per il mancato adeguamento del quale, come è noto, sono previste anche sanzioni penali; l'Art. 1 del Codice, infatti, mira a garantire "il rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

3. Il concetto di sicurezza

A differenza di qualche tempo fa, la sicurezza oggi non è più considerata come onere economico ma come investimento: essa va intesa non limitando l'interesse alla sola protezione del patrimonio informativo automatizzato contro rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali che siano, ma va intesa inglobando anche la limitazione degli effetti causati dall'eventuale occorrenza di tali cause: essa soprattutto si spinge oltre gli aspetti squisitamente tecnici, comprendendo anche aspetti organizzativi, sociali, culturali e legali. Un sistema informativo automatizzato, per essere ritenuto "sufficientemente" sicuro deve soddisfare alcune proprietà:

- disponibilità del dato: le informazioni ed i servizi che un sistema eroga devono essere a disposizione degli utenti del sistema stesso compatibilmente con i livelli di servizio stabiliti;
- integrità del dato: le informazioni ed i servizi possono essere creati, modificati o cancellati solamente dalle persone autorizzate ad espletare tali operazioni;
- autenticità: deve esistere la garanzia e la certificazione della provenienza dei dati;
- riservatezza: l'informazione può essere fruita solo dalle persone autorizzate a compiere tale operazione.

La sicurezza di un sistema non può essere intesa come qualcosa di

statico, essa diversamente è un processo continuo che coinvolge tutte le componenti di un'organizzazione e comporta il progetto, la pianificazione, l'implementazione, l'applicazione e la gestione di opportune contromisure di natura fisica, logica ed organizzativa. Occorre elaborare ed articolare dunque un progetto completo attraverso una serie di attività che vanno dalla definizione delle politiche di sicurezza alle regole comportamentali, dall'assessment all'analisi e alla gestione del rischio, dal piano operativo all'audit ed alla formazione del personale. Concretamente l'analisi del rischio si traduce nell'applicare una metodologia standard che possa definire le minacce, le vulnerabilità, i rischi che sono elementi fondamentali all'organizzazione per individuare le salvaguardie più adeguate e più convenienti.

Ai fini di una più corretta definizione degli ambiti, va specificato che:

Per rischio si intende la possibilità di avere una perdita oppure un danno o meglio l'eventualità che una minaccia possa trasformarsi realmente in danno comportando così un determinato impatto.

La minaccia invece viene definita come un evento di natura dolosa o accidentale che, sfruttando una vulnerabilità del sistema, potrebbe provocare un danno.

La vulnerabilità infine rappresenta una debolezza, ossia la facilità di avere una perdita, relativamente ad un dato bene, al concretizzarsi di una minaccia specifica per il bene stesso.

La salvaguardia è una contromisura consistente nelle azioni da intraprendere per ridurre il livello di vulnerabilità esistente in relazione al concretizzarsi di una minaccia per un dato bene. Le salvaguardie non necessariamente sono misure di sicurezza tecniche o fisiche ma investono tutta l'organizzazione.

4. L'analisi dei rischi

Prima dell'avvio delle fasi operative dell'analisi, è necessaria una prima attività di pianificazione dell'analisi stessa con lo scopo di definirne l'ambito e acquisire ogni elemento già disponibile e rilevante ai suoi fini. Nello stesso tempo occorre acquisire consapevolezza sul livello di esposizione al rischio del proprio patrimonio ed avere una mappa preliminare dell'insieme delle possibili contromisure da realizzare. Le fasi di questa attività sono riconducibili a:

- 1) identificare i beni da proteggere e le principali minacce: le risorse coinvolte sono quelle hardware (C.P.U., terminali, workstation, postazioni di lavoro, stampanti, ecc.) le cui principali minacce sono i malfunzionamenti dovuti a guasti, sabotaggi, ed eventi naturali come i terremoti, gli incendi e allagamenti, e furti di intercettazioni; quelle software (dei sistemi operativi, di base, applicativo, ecc.) le cui principali minacce sono legate, piuttosto, all'uso e cioè presenza di errori involontari commessi in fase di progettazione e/o

implementazione che consentono ad utenti non autorizzati di eseguire operazioni e programmi riservati invece che a determinate categorie degli stessi, presenza di codice maligno volontariamente inserito in modo tale da poter svolgere operazioni non autorizzate sul sistema o per danneggiare il sistema stesso (virus, Trojan, backdoor, ecc.), attacchi di tipo DOS Denial of service - (attacchi non distruttivi miranti alla saturazione delle capacità di risposta di un servizio che diventa, in tal modo, inutilizzabile); dati (contenuti di archivi, basi di dati, copie storiche, file di log, ecc.) le cui minacce sono legate alla debolezza dei sistemi operativi e delle applicazioni che operano sulle macchine su cui risiedono e sono riconducibili ad accessi non autorizzati, a modifiche volute o accidentali; risorse professionali (amministratori di sistema, gestori di rete, sistemisti analisti, programmatori, personale di manutenzione hardware e software) le cui principali minacce sono la distruzione o l'alterazione per opera di eventi naturali (e/o di azioni accidentali o intenzionali);

- 2) Classificare i beni e valutarli: Questi beni così identificati e determinati, vanno classificati in funzione degli elementi di integrità, riservatezza e disponibilità. La valutazione dei beni è indispensabile per comprendere la loro funzione strategica all'interno del sistema, e per poter, successivamente, valutare il livello di esposizione al rischio. I criteri per la valorizzazione devono inoltre tenere conto del rischio per la sicurezza del paese, per la sicurezza dei cittadini, per l'interruzione e/o l'alterazione di un pubblico servizio, per la sottrazione o alienazione o danneggiamento del patrimonio pubblico;
- 3) Valutare le minacce e le vulnerabilità: è indispensabile individuare le minacce e le vulnerabilità a cui sono esposti i beni affinché si possa valutare l'esposizione al rischio. Le minacce, come categorie, sono riconducibili a diverse aree quali la penetrazione logica, la penetrazione fisica, la penetrazione nelle reti di comunicazione, i guasti delle apparecchiature, gli errori umani. Vulnerabilità e minacce devono essere classificate in termini qualitativi e poi correlate ai beni per l'individuazione degli impatti e per la determinazione della misura del rischio in relazione ai diversi servizi;
- 4) Individuare l'esposizione al rischio: il valore dei beni, il livello delle minacce, il livello di vulnerabilità forniscono la misura del rischio a cui è esposto il sistema. Normalmente per ogni minaccia vanno considerate le criticità relative ai singoli beni ed al servizio informativo nel suo complesso, in funzione degli impatti relativi agli elementi di integrità, riservatezza e disponibilità considerati;
- 5) Individuare l'insieme delle contromisure da adottare al fine di incrementare il livello di sicurezza. L'analisi del rischio si conclude con l'individuazione di possibili contromisure da adottare allo scopo di abbattere l'entità del rischio precedentemente individuata. Per ogni componente e per ogni minaccia occorre determinare il livello di

rischio ritenuto accettabile. Per quanto riguarda le contromisure per ogni minaccia occorre stabilire vulnerabilità, danno potenziale, probabilità dell'evento, rischio per l'organizzazione, costi di ripristino, priorità nell'implementazione di meccanismi di sicurezza, contromisure urgenti, ordinarie, future.

Va ricordato inoltre che l'analisi non va intesa come qualcosa di statico ma è inserita nel ciclo di vita della sicurezza ed è soggetta a processi di verifica e di aggiornamento.

5. La sicurezza informatica negli anni '90

Lo scenario informatico degli anni '90 era costituito soprattutto da minicomputer e workstation, il più delle volte collegate ad internet con un indirizzo IP statico. Gli intrusori agivano in un ambiente sostanzialmente omogeneo in cui i sistemi operativi Unix-like erano la grande maggioranza.

Agli inizi del decennio in Italia i principali utilizzatori della rete erano le università e i centri di ricerca, le reti locali erano ancora alquanto eterogenee e l'uso domestico di internet e del computer non era ancora così diffuso. Oltreoceano la scena era più varia, ai centri di ricerca, accademici o no, si affiancavano le grandi aziende.

I servizi disponibili sulla rete erano limitati essenzialmente alla possibilità di collegamento remoto ad altro sistema, al trasferimento di file e alla posta elettronica. Nonostante l'esperienza traumatica dell'attacco del novembre 1988, l'attenzione verso la sicurezza informatica - intesa come problematica a se stante degna di appropriati investimenti, anche nel settore della ricerca - era abbastanza limitata: l'approccio più diffuso era quello di ignorare il problema finché le circostanze non costringevano a prenderlo in considerazione.

L'insieme di questi due fattori (omogeneità dell'ambiente e scarsa attenzione delle vittime) contribuiva a formare una classe di attaccanti estremamente preparata contrapposta ad una classe di vittime molto spesso completamente indifese. L'attacco del resto finiva per essere in molti casi un virtuosismo tecnologico, volto più che altro a soddisfare il narcisismo degli attaccanti, che agivano peraltro nel contesto di un sostanziale vuoto legislativo (la prima legge italiana che configura specificatamente il reato di frode informatica è del 1993). L'attacco più diffuso era l'accesso non autorizzato con la conseguente compromissione del file delle password e dell'account di amministratore. In questa situazione il ruolo dei Cert (Computer Emergency Response Team) era soprattutto di sensibilizzazione e trasferimento tecnologico: gruppi di esperti di sicurezza white hat fornivano le proprie competenze a chi incappava nelle maglie degli intrusori.

Conseguentemente le segnalazioni ricevute dai Cert riguardavano soggetti del tutto impreparati in materia che chiedevano consulenze per allestire rimedi o anche solo per capire l'entità dell'incidente verificatosi.

Comprensibilmente una delle principali richieste di tali soggetti era la

riservatezza delle informazioni: nessuno di essi aveva piacere che fosse resa pubblica la propria inadeguatezza strutturale a rispondere agli attacchi verso i propri sistemi informatici.

6. Il boom di internet

A metà degli anni '90 lo scenario cambiò radicalmente grazie soprattutto a due fattori:

- 1) l'introduzione del world wide web;
- 2) la disponibilità di sistemi operativi UNIX-like open source come Linux e FreeBSD.

Il web venne immediatamente apprezzato come una modalità semplice ed efficace di condivisione delle informazioni e fornì a molti una ragione forte per connettersi a internet. La disponibilità a costi irrisori di sistemi operativi di buona qualità e in grado di gestire servizi in rete favorì la crescita della richiesta delle connessioni internet, costringendo i produttori di sistemi operativi proprietari a fornire i medesimi servizi. Nel contempo si diffusero gli Internet Service Provider, i fornitori di connettività alla rete - di cui fanno parte gli grandi Telecom nazionali e piccole società nate sull'onda del boom - le une e le altre spesso ugualmente impreparate ad affrontare i problemi di sicurezza cui espose la connessione ad internet.

Il risultato netto di tale trasformazione dal punto di vista della sicurezza informatica fu uno scenario completamente nuovo:

- grande varietà di ambienti e protocolli;
- diffusione della figura del provider che, pur fornendo connettività ai propri clienti, non aveva con essi alcun vincolo organizzativo;
- la gestione dei server smise di essere patrimonio dei soli operatori e sistemisti cresciuti nei centri di calcolo.

Pertanto nella giungla della tecnologia diventò più facile trovare uno spiraglio per scatenare un attacco e, per portarlo a termine, servirono meno competenze. Alla figura dell'attaccante degli inizi (un po' sfuggente ma affascinante per la competenza tecnica che vi si cela), si aggiunse quella dei cosiddetti script kiddies, i ragazzini che scaricavano dalla rete programmi preconfezionati per portare a termine attacchi anche alquanto sofisticati. Qualcuno si limitava a giocarci, qualcuno imparava.

Nel campo degli attacchi la novità che chiude il decennio di internet e apre il nuovo millennio è costituita dai cosiddetti attacchi Distributed Denial of Service (Ddos) che compromettono la disponibilità di un servizio sfruttando la complicità, spesso inconsapevole, di decine di macchine della rete. La sicurezza diviene quindi uno dei fattori abilitanti anche per quella nuova attività che prende il nome di commercio elettronico, assai diffuso negli Stati Uniti e ai suoi albori nel nostro paese.

7. La sicurezza informatica negli anni 2000

Il contesto odierno è di nuovo differente. Da un lato l'opera di sensibilizzazione ha avuto effetto e gli utilizzatori di sistemi informatici sono oggi molto più attenti alla loro sicurezza e alla tutela della privacy di qualche anno fa. Gli strumenti, tecnologici e giuridici, sono aumentati significativamente. D'altra parte l'eterogeneità e la complessità degli ambienti operativi è ulteriormente aumentata, aprendo nuove sottili possibilità di intrusione. La diffusione di connessioni radio (wireless) ha aperto nuovi fronti d'attacco di difficile difesa, in quanto intrinsecamente accessibili a tutti (broadcast communication).

La diffusione ormai capillare di prodotti open source e di prodotti commerciali immessi sul mercato ancora immaturi per battere la concorrenza su un tempo (che la connessione globale fa scorrere più rapidamente), ha abituato gli utenti all'idea di prodotti software sempre imperfetti, da mantenere continuamente con l'applicazione di patch. Ciò nonostante la maggioranza degli attacchi sfrutta comunque vulnerabilità ben note, ma a cui non si è posto ancora rimedio nella continua rincorsa tra attaccanti e difensori.

Oggi i pericoli per gli utenti di internet non sono affatto diminuiti, ma la società odierna è assai meglio strutturata per difendersi. In Italia, per esempio, dal 1999 esiste una Polizia Postale e delle Comunicazioni specializzata negli interventi legali a reati informatici. Le aziende sempre più spesso si dotano di esperti di sicurezza e di strutture organizzative atte a gestire le situazioni di attacco. I provider anche grazie alla presenza di norme specifiche sono sempre più abituati e disposti alla collaborazione con le forze dell'ordine nell'indagine dei reati informatici.

La stessa internet ha assunto una struttura molto più gerarchica, trasformandosi in una rete di isole ben protette e il più possibile inaccessibili dall'esterno (intranet e VPN).

8. I dati dell'Osservatorio sulla sicurezza e Criminalità ICT (OCI)

In un sondaggio di imprese e pubbliche amministrazioni effettuato nel 2003 da FTI – Sicurforum Italia, appare evidente il costante incremento degli attacchi rilevati nel periodo preso in esame, per quasi tutte le tipologie di attacco considerato. In particolare si rileva che la contaminazione da virus riguarda ormai la totalità dei soggetti considerati. La rilevanza assoluta del fenomeno virus è peraltro coerente non solo con l'esperienza quotidiana degli utenti e degli specialisti, ma anche con le rilevazioni condotte negli Stati Uniti da CSI-FBI.

Le tipologie sono molte e ai virus di prima generazione nel tempo si sono aggiunti worm, Trojan, ed altri codici maligni che si replicano in rete con le vulnerabilità individuate nel software. Tale ultima generazione di virus viene definita malware, contraendo la locuzione malicious software.

Il fattore più critico è che internet - annullando le distanze e il tempo- , offre un vantaggio temporale a chi attacca, penalizzando invece chi deve difendersi. E' dimostrato che quando un worm si propaga all'estero raggiunge

l'Italia nei giorni e nelle ore successive.

I recenti virus non si trasmettono più solo attraverso i supporti magnetici (floppy, CD-Rom, ecc) con il fine di danneggiare file e settori di boot, ma sono diventati codici pericolosi in rete che si azionano a condizione che il sistema individuato offra una vulnerabilità da sfruttare e sulla quale innescare gli effetti nocivi.

Per le aziende e gli utenti in genere, emergono perciò due diverse tendenze e criticità: la prima riguarda i computer non protetti che potenzialmente sono vulnerabili a tutto, sia agli innumerevoli virus fino ad oggi creati sia ai recenti worm; la seconda possibilità è che anche le aziende ben organizzate sulla sicurezza informatica potrebbero subire incidenti per effetto dei nuovi codici installati a causa delle vulnerabilità dei sistemi operativi o delle applicazioni.

Da una recente ricerca di Euros Consulting relativa all'anno 2002, risulta che le principali conseguenze delle infezioni subite dalle aziende segnalanti sono state, nell'ordine:

- perdita di tempo e/o di produttività: 27%;
- pc non disponibili agli utenti 17%;
- Ritardi nei tempi di risposta del sistema: 13%;
- Invio automatico ed inconsapevole di e-mail infette ad altri destinatari 13%;
- File corrotti 10%;
- Inutili messaggi video: 10%;
- Blocchi di sistema 7%;
- Altri danni 3%.

Per avere un'idea delle necessità sulla sicurezza informatica, è necessario conoscere in che modo, quando e perché i virus e gli altri codici pericolosi si diffondono e penetrano nei sistemi aziendali.

Per quanto riguarda la segnalazione o la rilevazione dell'attacco subito, si nota come spiacevolmente per il soggetto attaccato, in diversi casi l'attacco sia stato segnalato da partner di business o da problemi di funzionamento dei sistemi o da indisponibilità, distruzione o alterazione dei dati. Un dato positivo è quello che indica nel 40% (2002) delle segnalazioni il ruolo avuto dagli strumenti e dai sistemi informatici di rilevazione delle intrusioni detti IDS (Intrusion Detection System). Per quanto riguarda l'origine degli attacchi, si conferma largamente l'accesso esterno nel 75% dei casi come era già stato rilevato negli anni precedenti. Tale prevalenza è certamente dovuta all'incidenza del fenomeno virus, agli attacchi di tipo Denial of Service (D.O.S.) ed ai tentativi di accesso da parte di soggetti sconosciuti via connessione internet. Altre analisi evidenziano infatti che attacchi molto pericolosi provengono dall'interno dell'organizzazione, coinvolgendo personale che ben conosce le misure di sicurezza adottate e quali siano le informazioni più critiche o utili.

Tuttavia il fenomeno virus rappresenta di gran lunga il più preoccupante. Il furto di apparati informatici contenenti dati, la saturazione

delle risorse, gli usi e le modifiche non autorizzate sono pure molto rilevanti, mentre nell'ultimo periodo assume importanza il fenomeno dei Trojan.

E' inoltre in aumento la percentuale relativa a "pirateria e frode informatica" che connota l'abuso di risorse ICT dell'organizzazione per scopi diversi da quelli previsti, soprattutto da parte di soggetti interni. Esce rafforzata la tendenza a considerare la maggior parte degli attacchi subiti di tipo vandalistico-dimostrativo, tipica degli hacker e della frode. Sono limitate le motivazioni riferite allo spionaggio ed al furto di informazioni aziendali, mentre si confermano rilevanti sabotaggio e terrorismo, forse sull'onda emotiva dell'11 settembre.

In tutte le rilevazioni, in percentuale maggioritaria, chi ha subito l'attacco dichiara di non avere avuto danni conseguenti di alcun tipo. Questo dato può essere interpretato in modi diversi: da un lato si può affermare che i meccanismi di protezione attuati hanno espletato il loro compito, cioè l'attacco è stato rilevato ma le misure di sicurezza messe in campo ne hanno annullato l'effetto. Dall'altro si potrebbe ipotizzare che eventuali interruzioni di servizio o il tempo dedicato alla risoluzione di eventuali problemi non siano stati effettivamente percepiti come un danno.

Tra le misure di sicurezza adottate, software antivirus e dispositivi firewall sono i sistemi maggiormente diffusi, mentre ancora troppo scarsa rispetto alle necessità appare l'adozione di strumenti IDS, PKI (Public Key Infrastructure), VPN (Virtual Private Network) e crittografici. Ciò conferma ancora la limitata adozione di strumenti di sicurezza basati sull'uso della firma digitale, nonostante la legislazione pionieristica che il nostro Paese ha ormai da diversi anni.

Dal sondaggio effettuato sembra emergere un approccio tecnico-organizzativo progressivamente adeguato alle nuove sfide della sicurezza dell'informazione, un approccio che vede sempre più coinvolte l'alta direzione aziendale e di conseguenza l'intera struttura tecnico-amministrativa.

L'assenza di una politica complessiva di sicurezza ICT è infatti limitata al 15% degli intervistati. Si noti però che solo il 23% dei soggetti ha attivato politiche complessive di sicurezza che comprendono corsi di formazione specifici e correlati alle politiche avviate (che è il metodo in grado di assicurare maggiore forza nell'adozione delle politiche definite). Per poter valutare l'efficacia delle politiche di sicurezza, è poi importante conoscere se e come si realizzi l'attività di auditing sulle politiche stesse.

La tendenza verso la definizione di politiche consapevoli e pianificate per la sicurezza ICT sembra comunque emergere da questi dati e le parziali insufficienze riscontrate paiono soprattutto giustificabili con i tempi tecnici di realizzazione.

In conclusione sembra sia possibile evidenziare:

- la crescente minaccia alla riservatezza ed integrità del patrimonio informativo, acuita dai nuovi e sempre più complessi ambienti distribuiti basati sull'architettura di protocolli internet e dall'interoperabilità sempre più stretta tra sistemi di soggetti diversi;

- la continua crescita e la criticità del fenomeno virus, acuito dall'uso crescente della posta elettronica e dallo scambio di programmi in rete, con l'attivazione di applet ed agenti ostili nelle connessioni a siti web non sicuri o non sufficientemente presidiati in termini di sicurezza;
- un uso crescente ma ancora limitato di strumenti di prevenzione, di individuazione e di monitoraggio del livello di rischio e di sicurezza dei propri sistemi, con la spiacevole conseguenza di ignorare, in molti casi, il fatto di essere oggetto di attacco;
- una buona performance nei tempi di ripristino dei sistemi attaccati;
- una crescente predisposizione all'adozione di politiche globali attive e consapevoli di sicurezza ICT.

Pertanto, diversamente dai tempi in cui la sicurezza ICT era prerogativa dei tecnici dei sistemi informativi, ora vi è la necessità di passare alla fase "strategica" nella quale la percezione dei rischi ICT e la conseguente adozione di idonee politiche di sicurezza deve essere oggetto di valutazione da parte del massimo livello decisionale, anche per l'impatto economico-organizzativo che tali strategie implicano.

9. Il trattamento dei dati

Nell'evoluzione tecnologica a cui abbiamo assistito fino ad oggi e a cui assistiamo quotidianamente appare evidente lo spostamento del livello di competenza del problema sicurezza informatica: mentre fino a qualche decennio fa l'utilizzo di apparecchiature informatiche era riservato a pochissimo personale interno (esclusivamente tecnico), e quindi la responsabilità della continuità operativa e della riservatezza delle banche dati era compito di tecnici esperti del settore, oggi giorno l'enorme diffusione di personal computer - utilizzati dalla stragrande maggioranza del personale del pubblico impiego e non - ha fatto sì che aumentassero i rischi legati ad un trattamento poco attento al proprio patrimonio informativo, proprio a causa della maggiore disponibilità del dato.

Inoltre il problema sicurezza non è più legato semplicemente a disfunzioni o malfunzionamenti degli strumenti informatici (hardware o software), ma si è di recente spostato verso l'utente ultimo che spesso, a sua insaputa e per la sua inesperienza, si fa tramite del furto o il danneggiamento di importanti dati aziendali.

10. Lo standard ISO/IEC17799:2000

Uno degli strumenti di riferimento per la sicurezza informatica è rappresentato dalla norma ISO/IEC17799:2000: divenuto standard internazionale con il nome di ISO/IEC17799:2000, esso ha definito 127 controlli di sicurezza e svariati elementi di best practise. Tale standard, differenziandosi dai precedenti e proponendo lo schema del ciclo di Deming con le fasi plan (Pianificazione), do (esecuzione), check (controllo), act

(miglioramento), ha raggiunto altissimi livelli di applicabilità, sottolineando l'importanza di un'appropriate analisi dei rischi e la necessità di implementare solo i controlli rilevanti per la specifica realtà aziendale.

11. Il trattamento dei dati negli EE.LL.

Da un rapporto sulla sicurezza informatica effettuato nel luglio 2002 dall'Ancitel, è emerso che solo il 12% dei Comuni intervistati ha adottato sistemi di difesa derivanti da una valutazione complessiva dei rischi e di una vera applicazione delle policy di sicurezza, integrando le tecniche di firewalling con quelle di intrusion detection ed antivirus centralizzato.

Diversamente, il 48% dichiara di utilizzare almeno una delle due tecniche sopracitate, dimostrando un certo grado di attenzione al problema. Il restante 40% del campione indagato, conferma la preoccupante e diffusa tendenza a trattare operativamente le problematiche della sicurezza informatica con una poco chiara visione progettuale, assemblando così sistemi di sicurezza destrutturati.

Appare di conseguenza evidente come rispetto alle Pubbliche Amministrazioni Centrali, la Pubblica Amministrazione Locale soffra di un leggero ritardo nell'informatizzazione dei propri processi operativi, probabilmente dovuto alla minore disponibilità economica e una ridotta attenzione a tale settore. Tale ipotesi è supportata dal fatto che lo stesso decreto legislativo n° 39/1993 (Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche) sia destinato alle amministrazioni dello stato, agli enti pubblici non economici nazionali, mentre "le regioni, gli enti locali, sono destinatari di atti di indirizzo e di raccomandazioni".

Recentemente tuttavia, anche in applicazione del Codice in materia di protezione dei dati personali (Decreto Legislativo n° 196 del 30.06.2003) che istituisce l'obbligo della redazione del Documento Programmatico per la Sicurezza per chiunque gestisca dati personali, si è posta maggiore attenzione alle problematiche inerenti la sicurezza informatica (probabilmente anche i recentissimi scandali della fuga di dati anagrafici regionali – vedi Laziogate – e le intercettazioni telefoniche – vedi Telecom – hanno contribuito a porre l'accento su tale delicatissimo argomento).

Particolare attenzione si è rivolta al trattamento dei dati informatici: l'allegato B – Disciplinare Tecnico in materia di misure minime di sicurezza – dedica ampio spazio alla trattazione di tale argomento:

- sono previste precise modalità di sicurezza per il trattamento dei dati informatici, sia per il sistema di autenticazione informatica che per il sistema di autorizzazione;
- Il trattamento è consentito a chi è in possesso di credenziali di autenticazione (costituite da User ID e Password) oppure di un dispositivo di autenticazione (token), o di caratteristiche biometriche dell'incaricato eventualmente associate ad una parola chiave;

- E' necessario garantire la segretezza delle credenziali;
- La password è composta da almeno 8 caratteri ed è sostituita almeno ogni 6 mesi (tre mesi per il trattamento di dati sensibili) e non può essere assegnata ad altri incaricati, nemmeno in tempi diversi;
- La password è disattivata nel caso non sia utilizzata da almeno 6 mesi o nel caso di perdita della qualità che consenta all'incaricato l'accesso ai dati personali;
- In caso di assenza dalla postazione di lavoro, l'incaricato deve avviare lo screen saver;
- In caso di ambiti diversi, sono utilizzati sistemi di autorizzazione, individuati antecedentemente all'inizio del trattamento e periodicamente verificati;
- Sono utilizzati software contro il rischio di intrusione (tipo firewall o antivirus) aggiornati almeno annualmente (semestralmente per i dati sensibili);
- Il back up dei dati è previsto almeno settimanalmente;
- Entro il 31 marzo di ogni anno deve essere redatto il Documento Programmatico sulla sicurezza contenente informazioni sui dati trattati, la modalità del trattamento, l'analisi dei rischi, le misure preventive, le modalità di ripristino dei dati, la formazione effettuata agli incaricati.

In caso di trattamento di dati sensibili sono previste maggiori misure di sicurezza:

- l'accesso riservato con idonei strumenti elettronici;
- la custodia in locali ad accesso ristretto delle copie di backup;
- ripristino dei dati entro 7 giorni in caso di danneggiamento degli stessi;
- il trattamento dei dati sensibili deve essere necessariamente disgiunto da quello dei dati personali.

E' evidente che il trattamento dei dati negli EE.LL., piuttosto eterogeneo, comprende tutte le tipologie di dati: personali (relativi al personale dipendente, collaboratori, società esterne, ecc.), sensibili (certificati medici dell'utenza, del personale dipendente, cartelle cliniche dei pazienti, ecc.) e giudiziari (contenziosi in atto, pratiche legali, ecc.).

L'adeguamento al Decreto 196/2003 da parte degli EE.LL. ha comportato innanzitutto l'individuazione di un Titolare e di un Responsabile del trattamento dei dati, quest'ultima persona fisica di riferimento in caso di esercizio dei diritti in materia di trattamento dei dati; inoltre ha dato l'avvio ad una attenta analisi sulla sicurezza del trattamento del dato a cui si è prestata poca attenzione fino ad oggi.

12. L'analisi dei rischi

L'analisi dei rischi suggerita dal Codice risulta piuttosto particolareggiata: vengono esaminati i comportamenti degli operatori, gli eventi relativi agli strumenti, e gli eventi relativi al contesto.

13. I Comportamenti degli operatori

Tra i rischi legati al comportamento degli operatori, il più alto è sicuramente quello della carenza di custodia della password di accesso al sistema informativo; nella maggior parte dei casi si pone pochissima attenzione all'utilizzo della password e la stessa spesso viene condivisa tra più utenti (gestendo in comune uno stesso computer per esempio) ; inoltre ricordare diverse password (in caso di autorizzazione per l'accesso) può risultare difficoltoso ad alcuni utenti poco avvezzi a tali procedure (d'altra parte l'acquisto di sistemi tecnologici alternativi di accesso al sistema - ad esempio token, biometria, ecc. - per i loro costi elevati non sarebbe conveniente). Pertanto, confidando nella buona fede dei colleghi e ignorando i rischi di perdita/furto dei dati legati all'uso delle credenziali di autenticazione, spesso gli utenti (definiti ironicamente dai tecnici "utonti") finiscono per garantire un facilissimo accesso al sistema informativo ad hacker o agli stessi insider, che, sfruttando le tecniche di ingegneria sociale, possono avere accesso o danneggiare il patrimonio informativo dell'ente.

D'altra parte la ridotta esperienza acquisita da parte dell'utente e la sua formazione (spesso percepita semplicemente come obbligatoria) non consentono una garanzia contro la fuga o il furto di dati.

Inoltre spesso nelle procedure di trattamento dei dati (salvataggio, memorizzazione su diverso supporto, ecc.) può capitare un "errore umano": distrazione, scarsa memoria, poca disponibilità all'apprendimento possono causare arresti degli strumenti informatici, indisponibilità del dato, ecc.

In costante aumento è inoltre il fenomeno del phishing, ovvero il furto di informazioni sensibili, codici e password, rilevato soprattutto in ambito bancario, ma tendente anche a carpire informazioni sulla gestione del sistema informativo all'interno dell'Ente.

14. Gli Insider

Paragrafo a parte viene dedicato all'emergente rischio dei crimini commessi dagli insider (personale interno all'azienda): infatti è molto frequente il caso di dipendenti (o ex dipendenti) che danneggiano o distruggono intenzionalmente importanti dati aziendali; poiché conoscono approfonditamente il sistema informativo dell'azienda essendone gli utilizzatori "privilegiati", possono eseguire con più facilità degli hacker operazioni "proibite" di vario genere: frodi, furti di informazioni, cancellazione o alterazione di dati, utilizzo delle macchine per scopi privati, ecc.

Inoltre i crimini ad opera di dipendenti e dirigenti interni all'azienda difficilmente vengono denunciati alle forze di polizia. La bassa percentuale di reati denunciati è dovuta al fatto che molto spesso le organizzazioni vogliono tutelare la propria immagine pubblica, evitando pubblicità negativa e assicurandosi dei solidi legami con le organizzazioni sindacali.

I computer crime inside vanno così aumentando e, fatto rilevante, appaiono oltretutto poco riprovevoli agli occhi di chi li compie poiché non vengono ritenuti fatti socialmente gravi paragonati agli altri crimini (ad es.

violenti).

15. Eventi relativi agli strumenti

Come abbiamo visto nel paragrafo precedente, l'azione di virus è una delle azioni informatiche che provoca maggiori danni all'interno del sistema informativo o ai singoli client. Spesso mail personali o professionali si fanno tramite di invio di allegati o codici maligni che provocano fermo macchina ed indisponibilità del dato (nella maggior parte dei casi per alcune ore, ma è possibile anche alcuni giorni). Lo Spamming ("pubblicità spazzatura") inonda quotidianamente le caselle di posta elettronica (anche questo è purtroppo un fenomeno in costante crescita, pur esistendo software antisпам già da diverso tempo).

Inoltre, a causa delle ridotte disponibilità economiche, in alcuni casi l'hardware a disposizione degli EE.LL. è piuttosto vecchio e di modesto valore, le risorse tecnologiche (se ci sono) non vengono ottimizzate, e la manutenzione ordinaria è scarsa o addirittura nulla; in aggiunta il personale, come anticipato sopra, non essendo formato su particolari dettagli tecnici, tende ad utilizzare il client in maniera non adeguata, causando oltremodo inconvenienti di fermo macchina o indisponibilità dei dati.

Poiché inoltre il rapidissimo sviluppo tecnologico (sia a livello hardware che a livello software) non consente ai manager d'azienda di maturare esperienze organizzative sull'operatività delle risorse umane e la funzionalità dei processi gestionali interni, spesso i vertici aziendali si trovano impreparati ad affrontare esigenze di riorganizzazione dei sistemi informativi; si deve quindi far riferimento a consulenti esterni con competenze specifiche sulla sicurezza e sulla gestione dei processi aziendali interni. Oltre quindi alla carenza di competenze specifiche sull'organizzazione interna, è facile trovare Responsabili del trattamento dei dati (ex D.L. 196/2003) senza alcuna competenza specifica in questo settore (ad esempio Responsabile Ufficio Acquisti o altro): tale situazione fa sì che sia elevato il rischio di un trattamento poco accorto del dato con il conseguente danneggiamento o perdita dello stesso.

16. Eventi relativi al contesto

La sicurezza fisica (chiusura degli armadi, degli archivi cartacei, ecc.) è stata molto spesso trascurata confidando sulla buona fede dei colleghi e del personale ospitato presso la struttura dell'Ente; ancora oggi capita spesso di vagare nei pubblici uffici passando totalmente inosservati, con la possibilità di carpire dati e informazioni o peggio sabotare il sistema informativo attraverso i cavi degli armadi metallici (rack) lasciati aperti. Come viene sostenuto da più parti, "la sicurezza non è un obiettivo, è un processo" pertanto occorre investire in tale settore e iniziare a diffondere la cultura della sicurezza a tutti i livelli: non è infatti raro incontrare aziende in cui i sistemi informativi sono garantiti

dagli accessi esterni (con firewall, tecniche antintrusione, ecc.), mentre vengono adottate dalle stesse politiche di sicurezza interne inadeguate che vanificano gli sforzi organizzativi (questa gestione viene definita “sicurezza m&m’s”: dura fuori morbida dentro).

Altro grande limite è rappresentato dalla inadeguata gestione del backup: nel caso di una frammentaria organizzazione centralizzata dei software, è possibile che lo stesso venga lasciati sui client e che la responsabilità del loro salvataggio venga relegata all’operatore; copie di CD-Rom e DVD contenenti dati, quando ci sono, vengono lasciati incustoditi sulle scrivanie alle mercè di tutti.

Guasti temporanei alla rete elettrica o agli impianti di condizionamento possono altresì provocare perdita di danni al patrimonio informativo: un back up che non tiene conto di tali eventualità (e quindi non adeguato) può garantire il salvataggio solo di alcuni dati e non di altri, compromettendo l’integrità delle informazioni.

17. Le responsabilità del dipendente

L’uso delle apparecchiature informatiche da parte del dipendente deve essere disciplinato da norme certe, in quanto da comportamenti non leciti, anche inconsapevoli, possono derivare gravi conseguenze sia sul piano tecnico, come la perdita di dati, che su quello penale, nonché al contempo, problemi di immagine all’ente stesso.

In un eventuale contenzioso nei confronti del dipendente, quali interessi prevalgono, quelli dell’amministrazione (di controllo) o quelli del dipendente (di riservatezza)? La tipologia del rapporto di lavoro sussistente nelle PP.AA. risale al 1993 con il D.L. 29/1993 che ha sancito la contrattualizzazione del rapporto di impiego, cancellando la supremazia della pubblica amministrazione nei confronti dei propri dipendenti, per ricondurre le vicende del rapporto di lavoro al diritto comune. Da qui una serie di provvedimenti in materia, tra cui le varie leggi Bassanini (tra le ultime decreto della funzione pubblica del 2000) che hanno culminato con l’introduzione del D.L. 165/2001 contenente norme generali sull’ordinamento di lavoro alle dipendenze delle amministrazioni pubbliche.

L’art. 2, comma 2, del D.L. 165/2001 precisa infatti che i rapporti di lavoro dei pubblici dipendenti sono disciplinati: dal Codice Civile e dalle leggi speciali sul lavoro d’impresa, compreso lo Statuto dei lavoratori che trova integrale applicazione anche nel pubblico impiego; mediante la contrattualizzazione dei rapporti individuali di lavoro; l’art. 2 comma 3 del D.L. 165/2001 dichiara esplicitamente che i rapporti di lavoro sono regolati contrattualmente, mentre l’art. 40, comma 1, precisa che la contrattazione collettiva si svolge su tutte le materie relative al rapporti di lavoro.

Da questo excursus normativo, si evince pertanto che nel rapporto di lavoro della PP.AA. sono applicabili le medesime tutele previste nell’ambito del rapporto di lavoro privato. A queste vanno ad aggiungersi il DPR 318/1999 rivolto sia a soggetti pubblici che privati (che prevede l’obbligo di predisporre

misure minime di sicurezza per il trattamento dei dati personali); le linee guida del Cnipa del 1999 (Centro Nazionale per l'Informatica nella P.A.) per la definizione di un piano per la sicurezza informatica.

Pertanto in caso di contestazione nei confronti del dipendente, l'Ente pubblico farà riferimento al Codice Comportamentale e alle sanzioni disciplinari previsti rispettivamente all'art. 58 e 58 bis del Decreto legislativo 29 del 3 febbraio 1993, ripresi dal più recente Decreto Legislativo 30 marzo 2001 n° 165. Nel Decreto del Ministro per la Funzione Pubblica 28 novembre 2000 - Codice di comportamento dei dipendenti delle PP.AA. – all'Art. 1 c. 2 si evidenzia che “I contratti collettivi provvedono, a norma dell'art. 58bis, comma 3, del D.L. 3 febbraio 1993 n° 29, al coordinamento con le previsioni in materia di responsabilità disciplinare. Restano ferme le disposizioni riguardanti le altre forme di responsabilità dei pubblici dipendenti”.

Sarà quindi buona norma, al fine di evitare contestazioni e contenziosi in materia, adottare una politica trasparente, comunicando con estrema chiarezza al dipendente i limiti di utilizzo degli strumenti informatici assegnati per lo svolgimento delle mansioni attribuite, nonché i rischi derivanti da uno scorretto utilizzo sia sul piano della sicurezza del sistema informativo che sul piano della responsabilità penale. E' fondamentale quindi adottare uno specifico Regolamento Informatico aziendale che tuteli la P.A. sia da eventuali reati di cui all'art. 40 del C.P.P. in caso di illecito commesso all'interno dell'azienda da un proprio dipendente (download di file Mp3, navigazione in siti web non autorizzati, diffusione di virus, ecc.), sia da un illecito trattamento dei dati personali (ex Decreto Lgs. 196/03).

18. Pronunce giurisprudenziali

Recentemente sono state emesse sentenze particolarmente rilevanti dalla Corte di Cassazione in merito all'argomento: la Sezione del Lavoro (con sentenza n° 19554 del 13.09.2006) ha infatti giustificato il licenziamento di un dipendente che ha comunicato ad un ex collega le proprie credenziali di accesso per accedere alla rete aziendale, pur non essendo stato autorizzato dalla stessa: si è rinvenuta infatti in questo caso una forma di inadempimento talmente grave da consentire il licenziamento attuato dalla società in questione; in altro caso, la Corte dei Conti - Sezione Giurisdizionale della Sicilia, con sentenza n° 390 del 02.03.2005 – ha ritenuto colpevole un dipendente della Agenzia delle Entrate che, avendo lasciato incustodita la propria postazione informatica, aveva prodotto una anomala procedura di sgravio. Il dipendente, pur non essendo l'autore materiale della irregolare procedura di sgravio, con il suo negligente comportamento “aveva prodotto una grave inosservanza delle disposizioni dettate dall'Agenzia sulle modalità di utilizzo del sistema operativo nell'ipotesi di temporaneo allontanamento dalla postazione di lavoro nella fase di trattamento di dati sensibili”.

Diversamente a Potenza, una sentenza della Corte dei Conti dello scorso marzo (83/2006/R) ha condannato due impiegati pubblici che avevano

utilizzato i personal computer d'ufficio per attività extracurricolari (installazione di un applicativo specifico per emettere fatture relative ad interessi personali) e navigazione a siti web pornografici. In particolare, il primo impiegato, a seguito dell'installazione dell'applicativo sopra descritto, aveva provocato la diffusione nella intranet aziendale di un particolare genere di worm, causando il fermo del sistema per un intero mese; è da segnalare che lo stesso, per il fatto di essere "tecnicamente competente" è stato riconosciuto maggiormente colpevole rispetto al collega, al quale, per la navigazione a luci rosse, invece è stato richiesto un risarcimento per ogni ora di navigazione effettuata.

Particolare altresì è la tesi dei due impiegati sulla responsabilità dell'accaduto: i due infatti sostengono che non possa essere provato il fatto che siano stati loro a compiere dette azioni: la Corte ha respinto tale tesi, secondo cui la perizia tecnica su tempi e modalità di acquisizione dei file infetti e sulla navigazione web ha dimostrato una causalità diretta; inoltre rimane comunque la responsabilità personale per il pc in dotazione che avrebbe dovuto, come previsto dalle regole, essere protetto da password di accesso.

19. Conclusioni

Nel clima di allarme permanente che si è determinato sul piano geopolitico e sociale e in una situazione nella quale la Rete assomiglia sempre più alla caotica situazione del traffico statale, nel quale comportamenti scorretti o inconsapevoli mettono a rischio anche coloro che adottano misure di sicurezza prescritte e necessarie per abbassare la propria soglia di rischio, la sicurezza ICT non è dunque tema semplice da affrontare, anche per la relazione con la tutela della riservatezza dei dati personali che lo pone in diretta connessione con il livello di democrazia e partecipazione delle nostre società. Ma occorre che tutti gli operatori attuino politiche e iniziative per la sicurezza ICT in modo da rendere possibile uno sviluppo affidabile e condiviso della e-society, che altrimenti non potrà realizzarsi con successo, né dal punto di vista economico, né dal punto di vista sociale.

CAPITOLO VIII

RINA LANCELOTTI

LE INTERCETTAZIONI: IMPLICAZIONI PER GLI OPERATORI DI TELEFONIA MOBILE

SOMMARIO: 1. Considerazioni introduttive. – 2. Delle intercettazioni in generale: definizione e profili di legittimità. – 3. Intercettazioni telefoniche e prestazioni obbligatorie. – 4. Conclusioni.

1. Considerazioni introduttive

Le inchieste basate sulle intercettazioni telefoniche che hanno recentemente coinvolto una pluralità di ambiti (da quello bancario, a quello calcistico a quello dello spettacolo) tra le quali da ultima rileva quella relativa alle intercettazioni illegali che ha interessato il settore security di Telecom - che ha portato agli arresti di 20 persone (dirigenti della società di telefonia ma anche poliziotti, militari della Guardia di Finanza e carabinieri) e per la quale, secondo i pm milanesi, era stata archiviata un “*enorme mole di informazioni e dati riservati, illegalmente ottenuti*”, ha comportato un sempre maggiore interesse dell’opinione pubblica su questo tema.

Il presente scritto ha lo scopo di analizzare la disciplina delle intercettazioni, considerata nella prospettiva delle implicazioni per i soggetti sui quali queste si ripercuotono ossia degli operatori di telefonia.

L’esperienza da me svolta nel settore delle telecomunicazioni presso la società H3G S.p.A (nel dipartimento Business security - privacy) mi ha dato modo di approfondire l’argomento specie dal punto di vista delle c.d. prestazioni obbligatorie, disciplinate dall’art 96 del Codice delle comunicazioni elettroniche (L. 259/’03), ossia di quegli adempimenti che gli operatori telefonici devono ottemperare a fronte di una richiesta posta in essere dalle competenti autorità giudiziarie.

Cercherò al riguardo di analizzare in primo luogo cosa si intenda per intercettazioni, e più nello specifico di esaminare la distinzione tra acquisizione legittima ed illegittima alla luce di quanto disposto in materia dal codice di procedura penale, e, successivamente di delimitare l’ambito materiale e le modalità tecniche con le quali, secondo quanto disposto dalla disciplina vigente in tema di prestazioni obbligatorie, le richieste di intercettazioni poste dall’autorità giudiziaria vengono evase.

Particolare interesse è stato inoltre da me rivolto alla disciplina riguardante le intercettazioni di comunicazioni alla luce del delicato contrasto tra le esigenze investigative proprie della giustizia penale e quelle di tutela del diritto alla riservatezza.

Sul tema ho potuto notare come tale contrasto diventi ogni giorno più acuto con l'avanzare del progresso tecnologico che, da un lato, esalta le potenzialità positive per lo sviluppo delle indagini offerte dalle intercettazioni delle comunicazioni e, dall'altro, pone in rilievo le capacità intrusive di questo strumento nella vita privata dei cittadini, anche di quelli totalmente estranei al procedimento penale.

La Corte costituzionale¹⁵⁴, sul tema, ha già posto il problema statuendo che si debbano tutelare e contemperare due distinti interessi: quello inerente alla libertà e alla segretezza delle comunicazioni nell'ambito dei diritti inviolabili della personalità previsti all'articolo 2 della Costituzione e quello connesso all'esigenza di prevenire e reprimere i reati, anche in base ad un oggetto di protezione costituzionale.

Al riguardo, infine, ho posto in evidenza le modalità con le quali H3G S.p.A., a fronte della richiesta di intercettazioni posta dalla competente autorità giudiziaria, tutela il diritto alla riservatezza dei propri utenti nel rispetto di quanto disposto dalla normativa in tema di trattamento dei dati personali, nonché le possibili risoluzioni ipotizzabili in tema di sicurezza delle intercettazioni telefoniche.

2. Delle intercettazioni in generale: definizione e profili di legittimità

Per intercettazione si intende comunemente la captazione clandestina di una comunicazione o conversazione riservata, posta in essere mediante l'impiego di strumenti meccanici o elettronici da un soggetto terzo rispetto agli interlocutori¹⁵⁵.

Essa può avere ad oggetto conversazioni e comunicazioni telefoniche, informatiche, telematiche o ambientali ed è sottoposta a numerose limitazioni attesa la necessità di rispettare le garanzie costituzionali cristallizzate dagli artt. 14 e 15 della Costituzione. La Legge Fondamentale, infatti, nello statuire l'invio della corrispondenza e di ogni altra forma di comunicazione, ne prevede la comprimibilità esclusivamente a fronte di un atto motivato da parte dell'autorità giudiziaria, adottato con le garanzie stabilite dalla legge.

L'intercettazione, così definita, è un'attività che dunque può essere compiuta legittimamente soltanto allorché sussistano determinati presupposti e su iniziativa di soggetti specifici.

L'art. 271 comma 1 c.p.p. ne determina, a contrario, i presupposti oggettivi stabilendo i casi in cui le intercettazioni telefoniche non possono essere utilizzate ossia prevedendo che *“i risultati delle intercettazioni non possono essere utilizzati qualora le stesse siano state eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli artt. 267 e 268 commi 1 e 3”*.

¹⁵⁴ Sentenza 63/1994 su www.cortecostituzionale.it

¹⁵⁵ Roberto Pirro - www.giustizia.it – intercettazioni la natura e i limiti

E' poi lo stesso codice di procedura penale a prevedere ed a disciplinare più dettagliatamente, tra i mezzi di prova esperibili, al titolo III capo VI, "le intercettazioni di conversazioni o comunicazioni" (artt. 266 e ss. c.p.p.)

La disciplina in esame abbraccia, come premesso, sia le "conversazioni o comunicazioni telefoniche e di altre forme di comunicazione" (art. 266 c.p.p.) che i "flussi di comunicazioni relativi a sistemi informatici o telematici" (art. 266-bis c.p.p.)

Trattasi di mezzo di prova esperibile solo relativamente a determinati reati gravi o che, per loro natura, presuppongono come elemento materiale dell'illecito l'utilizzo di mezzi di comunicazione.

Più specificamente l'art. 266 comma 1 c.p.p. dispone testualmente che *"l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati:*

- a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni e determinata a norma dell'art. 4;*
- b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'art. 4;*
- c) delitti concernenti sostanze stupefacenti o psicotrope;*
- d) delitti di contrabbando*
- e) reati di ingiuria, minaccia, molestia o disturbo alle persone col mezzo del telefono;"*

Fermi restando i presupposti oggettivi stabiliti dal precedente art. 266 nonché dall'art. 266 bis del codice di procedura penale, limiti soggettivi alla legittimità dell'intercettazione sono consacrati nel successivo art. 267 c.p.p. il quale statuisce che questa è legittima quando sia autorizzata dal Giudice per le Indagini Preliminari con decreto motivato, su richiesta del pubblico ministero, qualora vi siano dei gravi indizi di reato e sussista il presupposto dell'indispensabilità ai fini della prosecuzione delle indagini. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio ai fini della prosecuzione delle indagini, è lo stesso pubblico ministero a disporre l'intercettazione con decreto motivato, salvo la necessità della convalida dell'atto entro 48 ore dal giudice per le indagini preliminari ai fini dell'utilizzabilità. La convalida quale presupposto necessario all'utilizzabilità deriva proprio dalla riserva di giurisdizione stabilita in materia dalla Costituzione.

Al di fuori delle ipotesi di cui innanzi, l'intercettazione è illegittima e come tale inutilizzabile.

Al riguardo, di recente, la L. 20 novembre 2006 n. 281 che ha convertito il D.L. 22 settembre 2006 n. 259 - recante disposizioni urgenti per il riordino della normativa in tema di intercettazioni telefoniche - ha predisposto nuove misure che mirano a contrastare dell'indebita diffusione e

comunicazione di dati od elementi concernenti conversazioni telefoniche o telematiche illecitamente intercettate o acquisite, nonché di informazioni illegalmente raccolte.

Stabilisce tale legge - riformando l'art. 240 del c.p.p. (oggi relativo a documenti anonimi **ed atti relativi ad intercettazioni illegali**) ed inserendovi i commi 2, 3, 4, 5 e 6 - che il Giudice per le indagini preliminari dovrà disporre in tempi rapidi e certi la distruzione delle intercettazioni illegalmente acquisite, formate e raccolte, mentre il Pubblico ministero dovrà chiederne l'immediata secretazione. e la custodia; è stabilito altresì il divieto effettuare copia di tali atti, in qualunque forma e in qualunque fase del procedimento, e di utilizzarli¹⁵⁶.

La normativa di cui innanzi prevede altresì che, ai fini della conservazione della prova dei relativi dati, dovrà essere redatto un verbale delle operazioni di distruzione, con la sola menzione degli elementi descrittivi e il divieto di riportare il contenuto delle captazioni illecite. Il codice di procedura penale viene qui modificato nel senso di consentire nel dibattimento la lettura dei verbali di distruzione di cui sopra.

La legge n. 281/'06 ha inoltre introdotto una nuova fattispecie di reato in relazione all'illecita detenzione degli atti o dei documenti indebitamente detenuti; per tale reato è prevista infatti la reclusione da sei mesi a quattro anni, da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio.

Tale ultima fattispecie di reato integra quelle già previste dal codice penale, al libro II, titolo IX, capo III, sezione V, recante la normativa sui delitti contro l'inviolabilità dei segreti (art. 616 e ss.).

3. Intercettazioni telefoniche e prestazioni obbligatorie: fondamento normativo delle intercettazioni come prestazioni obbligatorie.

Alla disciplina "generale" in tema di intercettazioni nel procedimento penale si è affiancata, con l'emanazione del DPR n. 318/'97, una disciplina "speciale" per gli operatori di telecomunicazione. Tale Decreto, all'art. 7 comma 13, ha previsto che *"Le prestazioni effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie sono obbligatorie, non appena tecnicamente possibile da parte dell'organismo di telecomunicazioni nei tempi e nei modi che questo concorderà con le predette Autorità. Le prestazioni relative alle richieste di intercettazioni vengono remunerate secondo un listino, redatto per tipologie e fasce quantitative di servizi proposto dall'organismo di telecomunicazioni ed approvato dal Ministero delle comunicazioni in concerto con il Ministero di grazia e giustizia"*.

Le intercettazioni dunque, secondo la normativa suindicata, rientrano tra quelle prestazioni che l'operatore telefonico deve porre in essere a fronte delle richieste delle competenti autorità giudiziarie.

¹⁵⁶ altalex 22 novembre 2006 - www.altalex.it

Il fondamento di tale principio è oggi espressamente consacrato dal Codice delle comunicazioni elettroniche – Legge n. 259/’03 - che ha abrogato il dPR n. 318/’97 ed all’art. 96 ha previsto che :“ *1. le prestazioni a fini di giustizia effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie sono obbligatorie per gli operatori; i tempi ed i modi sono concordati con le predette autorità fino all’approvazione del repertorio di cui al comma 2*”.

“2. le prestazioni relative alle richieste di intercettazioni sono individuate in un apposito repertorio nel quale vengono stabiliti le modalità ed i tempi di effettuazione delle prestazioni stesse, gli obblighi specifici, nonché il ristoro d i costi sostenuti. La determinazione dei suddetti costi non potrà in nessun caso comportare oneri aggiuntivi a carico del Bilancio dello Stato rispetto a quelli derivanti dall’applicazione del listino cui al comma 4. Il repertorio è approvato con Decreto del ministro delle comunicazioni, di concerto con i Ministri di giustizia e dell’interno da emanarsi entro centottanta giorni dall’entrata in vigore del Codice”

La disposizione in esame non sembra, almeno apparentemente, innovare in modo significativo quanto previsto dalla disciplina previgente stabilita dal d.P.R. n. 318/’97 e ciò in primo luogo perché la norma conferma il carattere obbligatorio delle prestazioni rese a fronte di richieste delle autorità giudiziarie ed in secondo luogo poiché la norma ripete lo stesso schema di esecuzione della disciplina previgente, fondato su un atto di secondo grado che dovrà essere adottato dai Ministri interessati in concerto tra loro.

Il carattere di obbligarietà, che deriva direttamente dal decreto che dispone l’intercettazione ed autorizza le conseguenti operazioni di polizia giudiziaria ossia dai poteri attribuiti all’autorità giudiziariaa nell’ambito del procedimento penale, ha però, secondo il Codice delle comunicazioni elettroniche, delle conseguenze più stringenti per gli operatori. Lo stesso art. 96 del Codice, al comma 3, prevede, infatti, in caso di inosservanza all’obbligo, l’applicazione di un apparato sanzionatorio di tipo regolamentare non contenuto nell’abrogato d.P.R. n. 318/’97, ossia l’applicazione, in caso di inadempimento, dell’art. 32 commi 2, 3, 4, 5 e 6 del Codice delle Comunicazioni elettroniche il quale contempla la possibilità che, nel caso in cui tale inadempimento sia reiterato nel tempo e di particolare gravità, venga disposta nei confronti dell’operatore, dal Ministero delle Comunicazioni, la sospensione dell’attività per un periodo non superiore a due mesi od anche la revoca dell’autorizzazione generale alla fornitura di reti o servizi di comunicazione elettronica.

3a. Effettuazione in concreto delle intercettazioni da parte degli operatori.

In linea di principio l’esecuzione delle intercettazioni dovrebbe essere effettuata *“esclusivamente per mezzo degli impianti presenti nella procura della Repubblica”*. Qualora però tali impianti risultino *“insufficienti o inidonei ed esistono eccezionali ragioni di urgenza, il pubblico ministero può disporre, con provvedimento motivato, il compimento delle operazioni*

mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria” (art. 268 comma 3 c.p.p.)¹⁵⁷.

L'esecuzione delle intercettazioni telefoniche richiede quindi la cooperazione dell'operatore di comunicazione titolare delle numerazioni o comunque l'utilizzo impianti su cui dette numerazioni insistono materialmente.

In passato la collaborazione da parte dell'operatore si manifestava concedendo l'accesso fisico alle sue centrali agli operatori di polizia giudiziaria. Oggi, gli apparati di ultima generazione, dispongono di specifiche funzioni di intercettazione che, mediante operazioni di tipo logico, consentono di duplicare ossia di far ascoltare la comunicazione ad un soggetto terzo (centro di ascolto), in modo non percettibile ai soggetti intercettati.

Le attività di regola richieste agli operatori consistono nell'attivazione di tali funzioni e, laddove necessario, nell'assistenza all'attività di intercettazione svolta dagli operatori di polizia giudiziaria. Trattasi in particolare di declinare, con modalità sostanzialmente informatizzate, le richieste pervenute dall'autorità giudiziaria, tramutandole nei comandi macchina, che realizzeranno, in forma automatizzata e senza ulteriori interventi da parte dell'uomo, quanto necessario a fare in modo di replicare in tempo reale ed in maniera trasparente ed integrale il contenuto delle comunicazioni sottoposte ad intercettazione verso il centro ascolto indicato dall'autorità giudiziaria nel decreto autorizzatorio.

L'organizzazione del lavoro all'interno della struttura che fornisce le prestazioni obbligatorie si esplica nel seguente modo: le richieste provenienti dall'autorità giudiziaria, indirizzate alla direzione preposta per le prestazioni obbligatorie, pervengono a mezzo fax, posta elettronica o mediante consegna diretta; una volta ricevuto il decreto emesso dalla magistratura si procede ad una verifica di legittimità ed evadibilità ossia della rispondenza formale tra il contenuto decreto ed i dati relativi al c.d. bersaglio (numero di utenza da porre sotto intercettazione). Successivamente vengono predisposti i comandi con i quali viene effettuata la scelta delle opzioni necessarie per la realizzazione della duplicazione della comunicazione originata o ricevuta dal bersaglio verso il punto indicato nel decreto emesso dal Giudice per le indagini preliminari ovvero, in caso di urgenza, dal Pubblico Ministero.¹⁵⁸

Non vi sono elementi di mediazione tra i nodi di rete (che hanno sostituito le centrali operative dove materialmente insiste la comunicazione), il numero di utenza sottoposto all'intercettazione, ed i punti di ascolto, ciò significa che la comunicazione intercettata viene duplicata direttamente verso

¹⁵⁷ Piccola digressione che merita di essere effettuata riguarda la definizione di “impianti di pubblico servizio”; la norma del codice di procedura penale è stata adottata prima che fosse avviato il processo di liberalizzazione dei mercati ossia quando i servizi di telecomunicazione erano prestati solo da concessionari di servizio pubblico in senso proprio (cfr art. 1 Dpr n. 156/1973 per cui i servizi di telecomunicazione appartenevano in esclusiva allo Stato” parere fornito ad H3G S.p.A. dallo studio legale associato CLMV

¹⁵⁸ www.senato.it – resoconto stenografico della seduta parlamentare “indagine conoscitiva sul fenomeno delle intercettazioni telefoniche” tenutasi in data 12 settembre 2006.

il numero telefonico associato al centro di ascolto autorizzato dal Decreto emesso dal GIP.

Gli operatori hanno contezza esclusivamente dell'identità dei soggetti intercettati e dei dati tecnici afferenti le comunicazioni (ossia del numero di utenza da intercettare, del numero del centro di ascolto verso cui effettuare la duplicazione della conversazione e della durata dell'intercettazione).

La prestazione obbligatoria che l'operatore telefonico deve fornire ai sensi dell'art. 96 del Codice delle comunicazioni elettroniche risulta perciò esclusivamente strumentale all'attività posta in essere dalla polizia giudiziaria su autorizzazione del GIP non prevedendo alcuna attività operativa di registrazione, ascolto e trascrizione, del contenuto delle conversazioni sottoposte ad intercettazione “*fungendo da mero “ponte” tra il soggetto intercettato ed il centro di ascolto*”.¹⁵⁹

3b. Prestazioni obbligatorie e tutela dei dati personali dei soggetti intercettati – il provvedimento del Garante del 15 dicembre 2005.

Nell'ambito della tematica del rapporto tra le esigenze processual penalistiche alle intercettazioni e la tutela della privacy dei soggetti coinvolti, si pone in evidenza che, nell'attuale momento storico, le nuove tecnologie dilatano sempre più la capacità invasiva delle indagini penali.

Le indagini, oggi, hanno sempre più frequentemente ad oggetto non più solo il singolo fatto criminoso, ma anche interi fenomeni criminosi - quali a titolo esemplificativo il terrorismo, la criminalità organizzata, la corruzione - che risultano riferibili a un numero indefinito di persone, collegate tra loro tramite una serie di concatenazioni e di relazioni, che necessitano di essere seguite anche attraverso le intercettazioni.

I fenomeni di cui innanzi hanno comportato che, nei processi penali, emerga un'enorme quantità di dati, anche sensibili, riferibili ad un numero elevato di soggetti, molti dei quali del tutto estranei ai reati commessi ed alle indagini in corso.

Al riguardo la Corte Costituzionale, in riferimento alla fase delle indagini preliminari ed all'utilizzazione delle intercettazioni telefoniche a fini probatori disciplinata dall'art. 270 c.p.p., ha affermato l'eccezionalità di tale norma in quanto “*diretta a consentire l'utilizzazione in processi diversi di dette acquisizioni limitatamente ai casi in cui gli elementi raccolti risultino indispensabili per l'accertamento di delitti comportanti l'obbligatorietà dell'arresto in flagranza, indicati nell'art. 380 c.p.p.. Trattandosi di una norma legislativa incidente su un diritto di libertà individuale qualificabile come inviolabile ai sensi dell'art. 2 della Costituzione*” ed inoltre che “*l'incisione, attraverso l'intercettazione, nella sfera privata - tutelata come diritto costituzionale inviolabile - è infatti elemento sufficiente a giustificare il*

¹⁵⁹ Così Francesco Pizzetti alla seduta parlamentare “indagine conoscitiva sul fenomeno delle intercettazioni telefoniche” tenutasi in data 12 settembre 2006. su www.senato.it

diverso trattamento dei casi in cui tale incisione sia avvenuta da quelli in cui non sia occorsa. E' d'altronde indubbio - a prescindere dai suddetti profili di incostituzionalità - che la disposizione impugnata, nel contenuto su specificato, trova sicuro fondamento nella garanzia alla riservatezza delle proprie comunicazioni”¹⁶⁰

La “particolare delicatezza dei dati trattati con riferimento alla sfera personale degli indagati (e delle altre persone estranee alle indagini, ma coinvolte nelle comunicazioni e conversazioni) ed alla segretezza delle indagini”¹⁶¹ ed il sempre più frequente utilizzo dello strumento delle intercettazioni come mezzo di ricerca della prova da parte dell’autorità giudiziaria (dovuto in parte anche alla normativa posta in essere a fronte del contrasto al terrorismo internazionale)¹⁶², ha comportato che fosse posta l’attenzione sul tema, oltre che della Suprema Corte, anche del Garante per la Protezione dei Dati Personali; l’Authority, infatti, con il provvedimento del 15 dicembre 2005 ha previsto, in virtù dei suindicati presupposti, nuove misure di sicurezza presso gli operatori telefonici in tema di intercettazioni.

Il provvedimento del Garante del 15 dicembre 2005 è stato strutturato sulla base di precedenti accertamenti posti dalla stessa Authority nei confronti degli operatori di telefonia al fine di “verificare la liceità e la correttezza dei trattamenti dei dati in riferimento alla disciplina rilevante in materia di protezione dei dati personali, con particolare riguardo alle disposizioni a garanzia della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione”¹⁶³.

Osserva tale provvedimento che sebbene gli operatori non vengano in alcun modo a conoscenza dei contenuti delle intercettazioni in ogni caso raccolgono, selezionano, elaborano ed utilizzano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali questi comunicano. Trattasi in particolare di dati personali riservati che riguardano l’identità dei soggetti sottoposti ad intercettazione, l’arco temporale di svolgimento dell’intercettazione, i dati di traffico telefonico o telematico (data, ora, numero chiamato e durata della comunicazione) ed in alcuni casi anche i dati relativi alle chiamate entranti, ai tentativi di chiamata ed alla localizzazione geografica dell’utenza intercettata.

Nonostante che a seguito delle indagini effettuate il trattamento dei dati di cui innanzi fosse risultato legittimo, il Garante ha ritenuto in ogni caso necessario incrementare il livello di sicurezza rispetto ad alcune criticità allo scopo di tutelare la riservatezza delle informazioni prescrivendo agli operatori telefonici di adottare, entro 180 giorni dall’emanazione del provvedimento, alcune misure di sicurezza ultronee rispetto a quelle già adottate.

¹⁶⁰ Pronuncia della Corte Costituzionale n. 63/1994 su www.cortecostituzionale.it.

¹⁶¹ www.garanteprivacy.it – Prescrizioni del Garante (art. 154, 1 c) del Codice) – 15 dicembre 2005 in Bollettino del n. 67/dicembre 2005

¹⁶² c.d. Decreto Pisanu d.l. n. 144/2005 convertito in legge il 1 agosto 2005

¹⁶³ cit. www.garanteprivacy.it – Prescrizioni del Garante (art. 154, 1 c) del Codice) – 15 dicembre 2005 in Bollettino del n. 67/dicembre 2005

Tali prescrizioni hanno avuto ad oggetto la forma ed autenticità dei decreti di inizio attività che pervengono ai fornitori, le modalità di invio e ricezione della relativa documentazione, la gestione dei profili di autorizzazione e l'attribuzione dei diritti di accesso alle risorse informatiche, anche con riferimento ai singoli incaricati.

Le misure, concretamente previste al punto 3 del provvedimento citato, sono state suddivise in tre macroaree riguardanti gli aspetti organizzativi della sicurezza, la sicurezza dei flussi informativi con l'autorità giudiziaria e la protezione dei dati trattati per fini di giustizia.

Più nello specifico, l'Authority, ha disposto l'individuazione più selettiva del numero degli incaricati designati a trattare i dati, la separazione fisica tra dati di carattere contabile e dati documentali prodotti nel corso delle attività svolte, l'adozione di procedure di autenticazione robuste per l'accesso informatico da parte del personale incaricato ai dati trattati anche attraverso l'identificazione biometrica (prescrizioni afferenti, gli aspetti organizzativi della sicurezza), l'adozione di sistemi di comunicazione con l'autorità giudiziaria basati su aggiornati strumenti telematici, tecniche di firma digitale, e posta elettronica certificata evitando l'uso di sistemi meno sicuri come ad esempio il fax (prescrizioni afferenti la sicurezza dei flussi informativi con l'autorità giudiziaria), la registrazione in appositi audit log delle operazioni compiute dagli incaricati, la maggiore protezione dei dati attraverso la cifratura, la cancellazione immediata dei dati dopo la loro comunicazione all'autorità giudiziaria (profili afferenti la protezione dei dati trattati per fini di giustizia).

Sul tema, il 13 luglio 2006 in Commissione parlamentare, l'Authority, nella persona del prof. Pizzetti, chiariva *“che sostanzialmente trattasi della pretesa che, quando perviene la richiesta dell'autorità giudiziaria di attivare l'intercettazione o acquisire qualunque altra informazione utile a fini di giustizia, tale richiesta sia conosciuta all'interno del gestore telefonico solo da un numero di addetti limitato, definito, individuato, che sia sempre tracciabile il comportamento tenuto per corrispondere alle richieste dell'autorità giudiziaria e che siano immediatamente cancellati i dati raccolti per rispondere a tali richieste una volta che si siano soddisfatte... Si tratta di misure che in linea di massima chiamiamo di seconda generazione e cioè finalizzate anche a non rendere manipolabili successivamente i dati relativi al tracciamento dei comportamenti tenuti”*¹⁶⁴

L'inchiesta sulle intercettazioni telefoniche illegali che ha recentemente coinvolto il settore security di Telecom, nonché le precedenti inchieste che hanno coinvolto il mondo del calcio, dello spettacolo e bancario, hanno posto ancora più in risalto le criticità in tema di riservatezza e di sicurezza nella trasmissione dei dati.

¹⁶⁴ www.senato.it - resoconto stenografico della seduta “Indagine conoscitiva sul fenomeno delle intercettazioni telefoniche” tenutosi in data 13 luglio 2006.

Al riguardo il Garante per la protezione dei dati personali, sulla base del precedente provvedimento del 15 dicembre 2005, ha adottato, paventando un'ulteriore indagine più approfondita sul tema, in data 20 settembre 2006, disposizioni ancora più specifiche in tema di tutela della riservatezza delle intercettazioni prescrivendo, per ogni singolo operatore, delle misure ad hoc che dovranno essere adottate entro 90 giorni dalla data di notificazione dello stesso provvedimento.

3c. Il caso H3G

Al fine di ottemperare agli obblighi previsti dall'art. 96 del Codice delle comunicazioni elettroniche H3G S.p.A. ha istituito, sin dall'avvio della propria attività, la direzione "*business security*", strutturata su tre distinte aree di responsabilità: la prima, chiamata "*organizational e compliance security*" ha come obiettivo quello di garantire la compliance aziendale rispetto alla normativa vigente in tema di tutela della privacy; la seconda "*telecommunication and information security*" definisce ed elabora le linee guida in materia di sicurezza informatica; la terza "*operational security ed ARPO (Area Riservata Prestazioni Obbligatorie)*" gestisce la sicurezza di tutte le sedi H3G e le prestazioni obbligatorie.

L'area riservata alle prestazioni obbligatorie– ARPO - assicura il presidio dei rapporti di H3G con le autorità giudiziarie e di polizia per l'effettiva erogazione delle prestazioni richieste attraverso diverse operazioni. Più in dettaglio, si occupa di gestire e validare il rilascio delle informazioni alle autorità richiedenti, di definire i requisiti delle piattaforme dei sistemi dedicati a tale gestione e di effettuare materialmente la duplicazione delle chiamate entranti ed uscenti dell'utenza sottoposta ad intercettazione presso il centro di ascolto designato nel decreto autorizzatorio del giudice procedente.

All'interno dell'ARPO, che è un'area centralizzata presso un'unica sede, in ottemperanza con quanto disposto dal Garante per la protezione dei dati personali con il provvedimento del 15 dicembre 2005, le attività sono svolte settorialmente; ciò comporta che i soggetti responsabili per le intercettazioni non sono titolati a conoscere i dati afferenti le anagrafiche od i tabulati e viceversa.

Tutti i sistemi informatici che gestiscono le prestazioni obbligatorie sono dedicati e le aree in cui sono allocati i servers sono controllate e monitorate con un sistema di videosorveglianza e l'accesso alle stesse può essere effettuato solo con un particolare tipo di badge.

La prestazione dell'intercettazione è del tutto automatizzata e consiste, come già detto, nel duplicare il traffico telefonico in entrata e/o in uscita dell'utente (c.d. bersaglio) verso il punto di ascolto indicato nel decreto autorizzatorio. Gli operatori autorizzati hanno conoscenza dei dati tecnici delle intercettazioni (e non del loro contenuto), solo ed unicamente al fine di porre in essere le attività di predisposizione dei comandi che consentano di replicare le telefonate verso il punto di ascolto indicato.

Tutti gli operatori ARPO ai sensi del d.lgs 196/'03 sono nominati incaricati al trattamento dei dati e sono dotati di credenziali di autenticazione che vengono immediatamente inibite qualora non più in uso. Le operazioni effettuate vengono registrate in un apposito log di sistema che permette di associare ogni singola operazione svolta al soggetto che l'ha posta in essere.

I sistemi informatici sono protetti attraverso appositi firewall ed antivirus che vengono costantemente aggiornati ed i dati afferenti le intercettazioni (tecnici ed anagrafici) vengono interscambiati con le autorità autorizzate attraverso l'utilizzo di password e di sistemi di cifratura.

Si segnala sul tema che a seguito del provvedimento del Garante per la protezione dei dati personali del 20 settembre 2006, è in corso presso H3G un implementazione dei sistemi di sicurezza che prevede, tra gli altri, l'identificazione biometrica per l'accesso ai server ARPO in sostituzione dell'autenticazione effettuata attraverso l'immissione di user-id e password.

3d. Compensazione delle spese anticipate dagli operatori telefonici per la fornitura delle prestazioni obbligatorie

Altro argomento che merita di essere analizzato riguarda la disciplina relativa alle spese che gli operatori telefonici sostengono al fine di porre in essere le intercettazioni.

Tali spese sono considerate, dal nostro ordinamento, nella categoria residuale delle spese processuali "*straordinarie*", ossia delle spese diverse da quelle disciplinate espressamente e ritenute indispensabili dal magistrato che procede ad istruire la causa.

L'art. 96 comma 3 d.lgs. n. 259/'03 stabilisce espressamente che le prestazioni relative alle intercettazioni sono individuate in un apposito repertorio, approvato con decreto del Ministro delle comunicazioni in concerto con i Ministri di giustizia e dell'interno, in cui vengono stabiliti le modalità, i tempi di effettuazione e gli obblighi specifici a questi correlati nonché il ristoro dei costi. La disposizione prevede successivamente che tale repertorio non potrà in ogni caso importare "*...oneri aggiuntivi a carico dello Stato rispetto a quelli derivanti dall'applicazione del listino*" (concretamente tale listino risulta quello approvato dal Ministro delle comunicazioni con il decreto ministeriale del 26 aprile 2001 riguardante proprio la "Approvazione del listino relativo alle prestazioni obbligatorie per gli organismi di telecomunicazioni").

Il listino concernente le intercettazioni risulta tuttora in vigore nell'attesa che venga emanato il provvedimento sui canoni disposto dalla legge n. 311 del 2004, ossia la legge finanziaria del 2005, la quale modificando l'art. 96 del codice delle comunicazioni elettroniche ha prescritto che i tempi e i modi delle prestazioni obbligatorie siano individuati in apposito repertorio, approvato con decreto del Ministro delle comunicazioni di concerto con i Ministri della giustizia e dell'interno, mentre il ristoro dei costi sostenuto dagli operatori sia stabilito in un provvedimento sul canone approvato dal

Ministro della giustizia di concerto con i Ministri dell'economia e delle comunicazioni.

In materia vige dunque il principio secondo cui i servizi prestati dagli operatori telefonici alle autorità giudiziarie siano compensati secondo listini tariffari di uso corrente in ambito professionale che, per definizione, sono tali da garantire una adeguata remunerazione dell'attività svolta.

La funzionalizzazione dell'attività del privato alle esigenze di giustizia è certa nell'*an* ma non nel *quantum* del corrispettivo, restando quest'ultimo sottoposto alla disciplina pubblicistica di cui innanzi.

Tale disciplina, poiché applicata a liberi imprenditori, deve comunque consentire la copertura dei costi ed un ragionevole ritorno dei capitali investiti¹⁶⁵; *“la tesi dell'assoluta gratuità delle informazioni contrasta sicuramente con le regole tuttora vigenti in materia di giustizia penale... dalle quali si desume il principio che non possono essere posti a carico di terzi gli oneri da essi sostenuti allorché siano stati chiamati a rendere una prestazione collaborativi nell'ambito del procedimento penale”*¹⁶⁶

Nel rispetto dei principi indicati, il Codice delle comunicazioni elettroniche richiede, con esclusivo riferimento a prestazioni che abbiano carattere obbligatorio, la definizione di una tariffa cui dovranno fare riferimento i magistrati ex art. 168 del d.P.R. n. 115/2002 e ciò in virtù del generale potere dell'amministrazione di regolare le condizioni di accesso (anche c.d. speciale) alla rete (art. 42 del Codice delle comunicazioni elettroniche) in modo tale da consentire il recupero dei costi supportati dall'operatore (art. 50 del Codice delle comunicazioni elettroniche).

A titolo esemplificativo si rileva che l'attuale listino prevede che le intercettazioni telefoniche abbiano un prezzo al lordo dell'iva di circa € 246,00 al giorno.

Della prestazione effettuata viene successivamente emessa fattura; questa, in conformità con quanto previsto dal Garante per la protezione dei dati personali, con il provvedimento del 15 dicembre 2005 (che ha imposto al riguardo la separazione fisica tra dati di carattere contabile e dati documentali prodotti nel corso delle attività svolte), viene ad esistenza in un momento successivo (dopo circa un anno) e separatamente rispetto alla effettiva prestazione dell'intercettazione.

Ciò ha creato non pochi problemi agli operatori telefonici dappoiché la fattura, per essere liquidata dalla Procura, necessita che venga riprodotto in allegato il decreto omissato dal GIP che ha disposto l'intercettazione.

4. Conclusioni

¹⁶⁵ Così Consiglio di Stato sez. VI, 1 febbraio 2002 n. 567 in tema di concessionari di pubblici servizi.

¹⁶⁶ Così la sentenza del Tar Lazio n. 114/2001 in tema di concessionari di pubblici servizi.

Dall'analisi effettuata in tema di intercettazioni telefoniche risulta che il legislatore abbia cercato di mettere in sicurezza solo il tramite con il quale materialmente queste vengono effettuate.

Solo di recente, infatti, prendesi come esempio la Legge 20 novembre 2006 n. 281, si è posto di affrontare il problema della sicurezza anche presso le aule giudiziarie in modo da tutelare la privacy dei soggetti intercettati, la riservatezza delle indagini e di limitare la fuga di notizie.

La questione che si pone è quella che se da un lato il Garante per la protezione dei dati personali ha previsto delle misure di sicurezza stringenti c.d. "di seconda generazione" presso gli operatori telefonici, nulla ha disposto circa i soggetti che materialmente eseguono le intercettazioni e detengono i dati personali degli utenti intercettati.

Le procure che agiscono per conto dei giudici procedenti non sono a tutt'oggi dotate degli strumenti tecnologici idonei a rendere sicuro il passaggio delle informazioni. Si consideri che la maggior parte delle richieste di intercettazione, pervengono presso gli operatori attraverso fax intelligibili non crittografati.

I problemi attinenti la sicurezza della riservatezza dei dati riguardano soprattutto l'autorità giudiziaria; non si può non richiamare in proposito l'attenzione sugli effetti provocati dalla pubblicità conseguente al deposito, nelle forme previste dal codice di rito, di dati informativi raccolti ed elaborati per finalità giudiziarie.

Sotto questo aspetto, si rileva che la polizia giudiziaria non può che espletare le indagini che le vengono chieste e riferirne compiutamente l'esito, mentre il pubblico ministero ha l'obbligo, specificatamente sancito dalla legge, di deposito integrale di tutti gli atti a disposizione della difesa (artt. 291, 293 e 415 del codice di procedura penale). La circostanza che siano previste delle limitazioni alla possibilità di depositare tutto quanto sia stato raccolto e intercettato attraverso una selezione atta ad eliminare i dati ritenuti irrilevanti, da espletarsi davanti al giudice ed alla presenza delle parti, argina ma non risolve del tutto il problema. Si tenga conto anche che tutte le registrazioni afferenti le intercettazioni devono essere conservate, (solitamente su supporto cd-rom) fino al passaggio in giudicato della sentenza.

Sul tema bisogna considerare altresì che nella polizia giudiziaria operano, oltre ai gruppi di ascolto, i gruppi di analisi e quelli di trascrizione delle conversazioni; vi sono poi i cancellieri, i segretari e i magistrati cui vengono portate le trascrizioni ed infine, i difensori degli indagati. Un gran numero di persone, viene pertanto in possesso della trascrizione del contenuto di ogni intercettazione (alcune di queste, trascrizioni dovranno essere trasposte anche nelle richieste o nelle ordinanze di custodia cautelare essendo portate a conoscenza di altri soggetti). Rimane tra l'altro ferma la previsione di cui all'articolo 200 del codice penale, che dà facoltà al giornalista di non divulgare il nome della propria fonte.

Dal punto di vista degli operatori, sotto il profilo della sicurezza della riservatezza dei dati e della captazione delle conversazioni, una soluzione

ipotizzabile potrebbe essere quella di creare un data base unico cui le procure possano accedere attraverso una rete unica di comunicazione telematica.

Tale espediente garantirebbe infatti l'accesso esclusivo dei soggetti abilitati, la minore diffusione di materiale cartaceo, più facilmente riproducibile e diffondibile, e la minore possibilità che soggetti terzi possano inserirsi sui sistemi ed intercettare a loro volta siffatte informazioni riservate.

CAPITOLO IX

SANDRO CARBONI

IL PHISHING NELL'E-BANKING

SOMMARIO: 1. Phishing: “pescare informazioni private”. – 2. Unico disegno criminoso. – 3. E-Banking. – 4. Analisi, dati, previsioni.

1. Phishing “Pescare informazioni private”¹⁶⁷

In ambito informatico si definisce phishing una particolare tecnica di “cracking” utilizzata per ottenere l’accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l’utilizzo di messaggi di posta elettronica, opportunamente creati per apparire autentici.

Phishing si pronuncia come “fishing”, il verbo inglese “pescare”, e sta ad indicare una nuova tipologia di crimine informatico che, in questi ultimi tempi, si sta diffondendo sempre di più.

Questa azione criminosa consiste, infatti, nel “pescare” informazioni riservate di navigatori, soprattutto se ricorrono ai servizi di e-banking¹⁶⁸). Molti clienti di varie banche sparse in tutto il mondo, infatti, hanno constatato che i propri dati personali e bancari sono stati rubati attraverso falsi messaggi e-mail apparentemente provenienti dalle banche stesse.

In realtà si trattava solo di un sistema per far compilare dei moduli, chiedere i numeri dei conti e altre informazioni riservate ai clienti. Grazie a questi messaggi l’utente è ingannato e portato a rivelare dati sensibili, come numero di conto corrente, nome utente e password, numero di carta di credito ecc.

Il processo standard di queste metodologie di attacco può riassumersi nei seguenti passi:

1. l’utente malintenzionato “cracker”¹⁶⁹ spedisce all’utente vittima un messaggio e-mail (Elettronic mail) che simuli nella grafica e nel contenuto

¹⁶⁷ Si riportano qui i riferimenti bibliografici per una maggiore comodità del lettore: C.Pfleeger, S.Pfleeger, Sicurezza in informatica, Pearson Education Italia, 2004; W.Stallings, Sicurezza delle reti - applicazioni e standard, Addison-Wesley Italia, 2004; A.A.V.V. a cura di Giuseppe Cassano, Diritto delle nuove tecnologie dell’informazione e dell’Internet, Milano, Ipsoa, 2002; A.A.V.V. a cura di Roberta Mannucci, Lineamenti di informatica giuridica, Napoli Roma, ESI, 2002; Borruso Tiberi, L’informatica per il giurista dal bit a Internet, Milano, Giuffrè, 2001; Fugini, Maio, Plebani, Sicurezza dei sistemi informativi, Milano, Apogeo, 2001; Giannantonio Ettore, Manuale di diritto dell’informatica (seconda edizione), Padova, CEDAM, 2001; Sicurezza Informatica - (<http://www.sicurezzainformatica.it>); Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria - (<http://www.anssaif.it>); Il quotidiano di Internet dal 1996 - (<http://punto-informatico.it>)

¹⁶⁸ “e-banking”: è l’opportunità offerta a tutti gli utenti bancari di effettuare operazioni di visualizzazione dati bancari e di transazione monetarie attraverso la connessione internet.

¹⁶⁹ “cracker”: utilizzano svariate tecniche tra cui lo sfruttamento di bachi che un determinato sistema o programma può avere per entrare nei sistemi informatici e fare danni.

quella di una istituzione nota al destinatario (ad es. la sua banca, il suo provider web, un sito di aste online a cui è iscritto, ecc.);

2. l'e-mail contiene avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account ecc.(ad es. un addebito enorme, la scadenza dell'account ecc.);

3. nella e-mail il destinatario è invitato a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione;

4. il collegamento al sito web della banca fornito NON porta in realtà al sito web ufficiale, ma a pagine appositamente create che sono veri e propri cloni dei siti ufficiali nei quali si richiede al destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server e quindi finiscono nelle mani del cracker;

5. il cracker utilizza questi dati per trasferire somme di denaro o per acquistare beni. Eccone un classico esempio:

«Gentile Utente eBay, durante i regolari controlli sugli account non siamo stati in grado di verificare le sue informazioni.

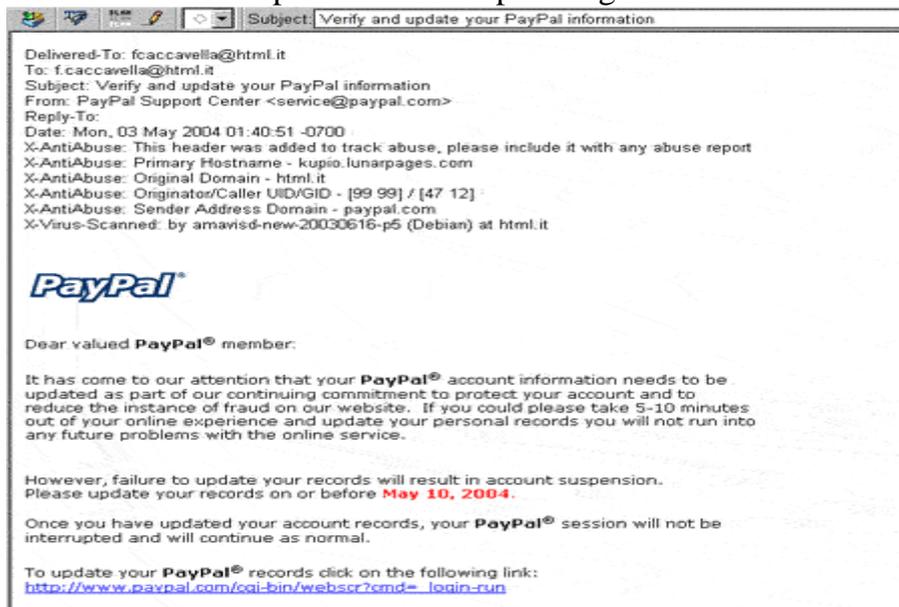
In accordo con le regole di eBay abbiamo bisogno di confermare le sue reali informazioni.

È sufficiente che lei esegua il login e completi il modulo che le forniremo.

Se ciò non dovesse avvenire saremo costretti a sospendere il suo account».

Questo è un esempio tradotto di phishing, il sistema illegale di raccolta di informazioni sensibili, dati di carta di credito e password che è stato utilizzato da molti cracker nell'ultimo periodo.

Ecco un altro esempio di e-mail di phishing arrivata a un indirizzo mail:



Il sistema è semplice, per riassumere, si inoltrano e-mail che paiono provenire da istituti di credito, da aziende che gestiscono siti Internet, dalle più svariate organizzazioni che richiedono dati personali agli utenti, millantando un rinnovo dei server.

L'e-mail vengono formattate in modo da contenere loghi di stile del tutto simili a quelli originali e i link indirizzano verso pagine web fittizie, completamente identiche alle pagine ufficiali (clonazione di pagine ufficiali). (Ad esempio, viene indicato l'indirizzo: www.bancaintesa.it/piu/mod/... L'indirizzo sembra relativo al dominio: www.bancaintesa.it, ma non è così: in realtà è www.bancaintesa.it/piu.mod/...).

I moduli che si troveranno in queste pagine (web) non hanno naturalmente nulla a che fare con quelli ufficiale imitate nelle e-mail e così le password e i numeri di carta di credito finiscono nella banca dati del truffatore che ha inviato la finta e-mail.

Precedentemente già è successo che qualcuno usa la rete per aggirare qualche povero navigatore, anche se i metodi sono decisamente cambiati.

2. Unico disegno criminoso.¹⁷⁰

Superata questa prima fase della truffa telematica, i phishers devono nascondere ogni traccia dei successivi trasferimenti di denaro dal conto del truffato, attraverso complesse operazioni bancarie per così sviare le possibili indagini della polizia postale.

Tale tecnica viene effettuata attraverso una complessa serie di trasferimenti bancari, avvalendosi di altri utenti complici, ma non consapevoli. Questi trasferimenti avvengono promettendo opportunità di guadagno e/o lavoro ad altri. Infatti, gli aspiranti lavoratori, ignari di quanto stanno compiendo, permettono ai phishers di far depositare, per qualche tempo, determinate somme di denaro per poi trasferirle presso altri conti con lo scopo, come precedentemente detto, di far perdere le tracce informatiche.

Queste operazioni, ovviamente avvengono in cambio di un corrispettivo, generalmente calcolato sulla percentuale del valore delle somme depositate e poi trasferite.

Obiettivo primario per il phisher è quello di fare transitare tali somme su molteplici conti correnti finché non vengano poi inviate all'estero o presso i fiduciari dei truffatori.

Il phishing si presenta come un fenomeno complesso è caratterizzato da profili sia civili che penali.

¹⁷⁰ A.A.V.V. a cura di Mario Jori, *Elementi di informatica giuridica*, Torino, G. Giappichelli, 2006; A.A.V.V. a cura di Roberto Tomei, *Il nuovo diritto*, Milano, Giuffrè, 2006; Claudia Pecorella, *Diritto penale dell'informatica*, Padova, CEDAM, 2006; Rosa Buonamassa, *Le fonti del diritto nel mondo dell'informatica*, Bari, Cacucci, 2006; A.A.V.V. *Diritto e società dell'informazione : riflessioni su informatica giuridica e diritto dell'informatica*, Milano, Nyberg, 2005; Giuseppe Cassano, *Diritto dell'Internet: il sistema di tutele della persona*, Milano, Giuffrè, 2005; Taddei Elmi Giancarlo, *Corso di informatica giuridica*, Milano, Simone 2003; Pascuzzi G., *Il diritto dell'era digitale: tecnologie informatiche e regole privatistiche*, Bologna, Il mulino, 2002; Giorgio Pica, *Diritto penale delle tecnologie informatiche*, Torino, UTET, 1999; A.A.V.V. *Attualità forensi*, pubblicazione a cura della "Fondazione dell'Avvocatura Italiana" presso il Consiglio Nazionale Forense Diritto & Diritti (<http://www.diritto.it>); *Giurisprudenza & Informatica* - (<http://legali.com>)

Importante è soffermarsi su quest'ultimo profilo: la legge non prevede una disciplina e una definizione specifica per il phishing, la quale si configura come una molteplicità di azioni finalizzate ad un unico disegno criminoso.

Il modus operandi dei phishers integra gli estremi di svariate ipotesi di reato previste dal codice penale e dal codice in materia di protezione dei dati personali (D.Lgs 196/2003):

- Truffa – art. 640 c.p.: "Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a perché o ad altri un ingiusto profitto con altrui danno, è punito[...]" - aggravante - "2) se il fatto è commesso ingerendo nella persona offesa il timore di un pericolo immaginario[...]"
- Trattamento illecito di dati – art. 167 D.Lgs n. 196/2003: "[...], chiunque, al fine di trarne per perché o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129 è punito, [...]"
- Accesso abusivo in un sistema informatico o telematico – art. 615 ter c.p.: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito[...] – aggravanti - [...]"
- Frode informatica – art. 640 ter c.p.: "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a perché o ad altri un ingiusto profitto con altrui danno, è punito[...]"
- Riciclaggio – art. 648 bis: "Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito[...]"

Gli articoli del codice penale e del codice in materia di protezione dei dati personali elencati in precedenza sono ravvisabili nella condotta dei phishers:

➤ applicazione dell'art. 640 c.p. – l'email fraudolenta contiene un collegamento ipertestuale ingannatorio (artifici o raggiri) che rimanda verso un sito clone dell'originario (induzione in errore) ed infine nel quale vengono sottratti i codici d'accesso della vittima che sono successivamente utilizzati per sottrarre il denaro (ingiusto profitto ed altrui danno). Cosicché, con quest'ultima azione del phisher si perfeziona il reato.

A volte nell'e-mail è presente anche il consiglio di recarsi repentinamente, ad esempio nel sito del proprio istituto di credito, prospettando rischi di truffe o altri accessi ai dati personali non consentiti (ingenerando nella persona offesa il timore di un pericolo immaginario). In quest'ultimo caso, ci sono gli estremi che integrano l'ipotesi di un'aggravante.

➤ applicazione dell'art. 167 D.Lgs 196/03 – Successivamente alla raccolta dei dati personali della vittima, che automaticamente vengono registrati in un database, il phisher pone in essere un trattamento di tali dati in violazione del disposto dell'art. 11 D.Lgs 196/03 e in seguito con la condotta di trarne profitto, nel momento in cui il denaro viene sottratto, il phisher realizza un ulteriore illecito penale ex art. 167 D.Lgs 196/03.

➤ applicazione dell'art. 615 ter c.p. – il phisher accede all'account della vittima senza aver nessun titolo e così eludendo le misure di autenticazione e di identificazione predisposte dal sistema informatico per garantire la tutela dei dati in esso contenuti. Pertanto, l'accesso è abusivo e conseguentemente è accompagnato da una frode informatica (art. 640 ter c.p.).

Inoltre, se l'azione di phishing avesse causato il blocco anche momentaneo dell'accessibilità dell'utente presso il suo istituto di credito, in tale ipotesi ricorrerebbero gli estremi di un aggravante di codesto reato.

➤ applicazione dell'art. 640 ter c.p. – il phisher carpando i dati d'accesso della vittima, li utilizza nei rispettivi account intervenendo nei sistemi informatici, ad esempio dell'istituto di credito, senza aver alcun titolo (senza diritto, con qualsiasi modalità). In questa fattispecie, il reato è commesso contro l'istituto di credito colpendo il suo sistema informatico.

La Suprema Corte ha più volte ricordato che la differenza tra la truffa e la frode informatica è circoscritta solamente per ciò che concerne l'attività fraudolenta dell'agente che investe non la persona, bensì il sistema informatico, infatti la struttura e gli elementi costitutivi di questi due reati rimangono inalterati.

➤ applicazione dell'art. 648 bis c.p. – infine, dopo aver sottratto illecitamente il denaro dai conti correnti delle vittime, gli autori dei reati ne compiono uno ulteriore con la realizzazione di tale ulteriore attività si configura il reato di riciclaggio.

I phishers, per trovare utenti disposti a far transitare per breve tempo somme di denaro di illecita provenienza, utilizzano varie società su Internet che permettono facili guadagni.

Il lavoro richiesto è di una facilità estrema; infatti, non si deve far altro che incassare tali somme sul proprio conto corrente per poi inviarle su ulteriori conti correnti indicati dalla società stessa, in cambio di una percentuale sul denaro transitato.

Accettando tali offerte di lavoro online, vi è un forte rischio di essere coinvolti in processi per riciclaggio o perlomeno limitatamente nelle indagini preliminari.

Per non cadere nelle trappole del phishing, si devono seguire due consigli: il primo, è quello di non credere a messaggi elettronici che richiedano informazioni personali riservate o codici di accesso a conti correnti, perché tali richieste non perverranno mai via e-mail; il secondo, è quella di non credere a chi promette facili profitti chiedendo solamente la disponibilità del proprio conto corrente.

Una possibile tecnica di difesa potrebbe essere usare dei “filtri”: è una possibile soluzione anti-frode basata sulla tecnologia bayesiana¹⁷¹ già usata per i programmi anti-spam in modo tale da bloccare i messaggi prima che entrino in un’organizzazione.

Il vero obiettivo degli strumenti di difesa è in definitiva lo stesso degli anti-spam, ovvero determinare con sicurezza la fonte reale di una e-mail. Comunque, occorre ribadire che le società operanti via internet assicurano che mai chiederebbero ad un cliente di fornire in questo modo i propri dati, ma a volte l’abilità dell’impostore di falsificare le intestazioni e la scarsa informazione dell’utente provocano danni irreparabili.

Proprio per combattere la piaga delle truffe, eBay, una delle più famose case d’asta telematiche, ha creato un apposito sito dove chiede ai clienti di girare (ovviamente senza aprirle) le e-mail sospette, in modo da poter ricorrere successivamente alle autorità di polizia postale.

3. E-banking¹⁷²

La nascita e la diffusione sempre maggiore del phishing è strettamente collegata, alla nuova “era di Internet”, in cui avvengono trasformazioni radicali in tutti i settori economici, poiché l’utilizzo delle tecnologie dell’informazione, delle telecomunicazioni e dei mass media ha creato tutti i presupposti per nuove forme di business.

Un ruolo molto importante nella “New Economy” è ricoperto dalle banche e dagli altri istituti che prestano servizi finanziari online, infatti questi fungono da sostegno per le nuove imprese nascenti nell’era del web.

Tutto ciò comporta trasformazioni evidenti nel settore, così provocando cambiamenti profondi nelle imprese bancarie; peraltro questo processo sta investendo in generale tutta l’economia e successivamente si verificherà una significativa selezione degli operatori attualmente presenti. E coloro che sopravvivranno avranno caratteristiche molto diverse da come si presentavano fino a poco tempo fa.

In particolare, si ritiene che nel settore bancario lo sviluppo della rete e l’enorme aumento della connettività caratterizzanti la “Nuova Economia”

¹⁷¹ Questa tecnologia si basa sugli studi del matematico inglese Thomas Bayes che presentò il teorema di Bayes. Le applicazioni del teorema sono innumerevoli, infatti viene anche utilizzato nella realizzazione di sistemi di filtraggio impiegati nella lotta contro lo spam. E’ un metodo di filtraggio statistico ed usa metodi probabilistici per predire se un messaggio è spam, basandosi su raccolte di email ricevute dagli utenti. Il servizio analizza le parole che si trovano nell’oggetto dell’e-mail, la firma e il testo dell’e-mail e, in generale, la frequenza d’uso di ogni singola parola, impara e memorizza i criteri scelti dall’utente.

¹⁷² A.A.V.V. a cura di Maurizio Baravelli, Anna Omarini, Le strategie competitive nel retail banking: segmentazione della clientela, modelli organizzativi e politiche commerciali, Roma, Bancaria, 2005; Bracchi G., Francalanci C., Giorgino M., Internet Banking, Milano, Egea, 2000; Dainesi E., Netbanking, banche e utenti dialogano su Internet, Milano, Apogeo, 2000; Pecenic M., Web Banking - Indagine alla scoperta delle banche italiane in rete, Milano, Simone, 2000; Biffi A., Filotto U., Soluzione banca virtuale, SDA Bocconi-SMAU, Milano, 1997; Banca d’Italia (<http://www.bancaditalia.it>)

avranno l'effetto di cambiare in pochi anni le professioni, ad esempio quella dell'intermediazione finanziaria, molto più di quanto non sia accaduto negli ultimi secoli.

Le ragioni per adottare l'e-banking sono veramente numerose, tra le più importanti si ricordano:

- risparmio di tempo e di personale agli sportelli;
- eliminazione dei supporti cartacei con conseguente risparmio di costi;
- ottimizzazione del processo di gestione dei flussi finanziari;
- facilità di esecuzione delle disposizioni di incasso/pagamento;
- abbattimento della necessità di capillarizzare gli sportelli.

Inoltre, in seguito ai risultati di un'estesa indagine condotta su utenti che fruttano i servizi bancari, è emerso che, dal punto di vista della domanda, oltre il 90% degli intervistati ritiene che l'uso di Internet per i servizi finanziari rappresenti un risparmio di tempo nonché di denaro, e inoltre ritengono di poter ottenere anche un servizio qualitativamente migliore rispetto allo sportello.

Questo "Internet" non può semplicemente essere considerato una nuova tecnologia di successo, ma deve essere studiato come fenomeno in grado di influenzare l'intera economia.

Occorre, comunque, ricordare che agire solo online non è detto che sia una scelta vincente: nella maggior parte dei casi occorre integrare e coordinare azioni online e azioni più tradizionali, per ottenere un marketing bancario a 360 gradi che possa coinvolgere sia le tipologie di clientela più tradizionali che i segmenti che invece hanno una maggiore propensione all'uso delle nuove forme di comunicazione.

Le banche dovranno pianificare la giusta integrazione tra rete di vendita tradizionale, basata sugli sportelli e sulle filiali, e quella innovativa, basata su Internet e gli altri nuovi canali di comunicazione: da un lato, è stata traslata su Internet l'operatività di massa, quella più ripetitiva, così consentendo al cliente di effettuare in rete le operazioni risparmiando prezioso tempo che si era costretti a impiegare nelle lunghe file agli sportelli, inoltre, è possibile informarsi su diverse tematiche, fare simulazioni, raccogliere documentazioni, creare preventivi per prestiti (ecc.); dall'altro lato, è stato rivisto il ruolo delle filiali e degli sportelli, allo scopo di alleggerire l'operatività di massa e lasciando invece inalterata la consulenza e la chiusura fisica delle operazioni. In questo modo il cliente ha un sistema, offerto da un'unica banca, che supporti le sue esigenze e non è, ad esempio, più costretto a tenere due conti correnti separati, uno online e uno tradizionale.

In sostanza, anche se la banca preferisce spostare, per ovvie ragioni, la maggior parte dei servizi su Internet, il ruolo delle filiali e degli sportelli continua ad essere un compito attivo, poiché, come abbiamo appena visto, il servizio online non è sostitutivo della rete fisica, ma si può affiancare ad essa, che rimane il punto di contatto fisico con il cliente, il quale vi si reca soprattutto per ottenere servizi meno di massa, quindi più complicati e per concludere le operazioni eventualmente già concordate online.

Inoltre, non tutti i clienti di una banca sono disposti ad utilizzare i canali virtuali, infatti, frequentemente i clienti con maggior capitale sono in età più avanzata e non sempre vogliono o sono in grado di usare le nuove tecnologie, mentre i giovani hanno una maggiore propensione all'utilizzo di Internet.

Quindi i siti bancari devono comunicare nei modi più semplici possibili con il cliente, attuale o potenziale che sia, fornire aiuti in qualunque area di navigazione, e creare un'assistenza che sia tempestiva ed efficace e non lasci solo il cliente, soprattutto nei momenti di maggiore difficoltà.

In questo modo, anche il cliente con maggiori problemi e con minore propensione verso la nuova tecnologia può prendere confidenza sempre di più con la propria banca online ed arrivare ad utilizzarla quotidianamente per le proprie operazioni.

Ciò rende necessario, da parte della banca, investimenti in tecnologia e in risorse umane che garantiscano un buon grado di comunicatività con il cliente anche a dispetto della distanza.

È importante, quindi, che il cliente abbia la sensazione di essere seguito e aiutato laddove ne abbia necessità.

Infatti, l'utente non vuole perdersi nel sito della propria banca avendo la possibilità di poter far tutto, ma senza poi fare davvero nulla in conclusione. Meglio creare un vero e proprio sito complementare a quello bancario per alcune tipologie di servizi, completamente dedicato all'argomento, che il cliente percepisca come altro rispetto al sito tradizionale anche se sempre sotto il controllo e la gestione della banca.

In questo modo si fornirebbe al cliente la possibilità di lavorare su qualsiasi argomento, in modo indipendente e completo, a partire dalle sue reali esigenze.

Come si è già osservato, i servizi bancari offerti via Internet non si discostano molto dai servizi dell'offerta tradizionale, ma per certi aspetti sono più ricchi di contenuti e più facilmente usufruibili: si pensi, ad esempio, al listino titoli aggiornato ogni 15 minuti (pensate se si volesse sapere da una banca tradizionale la quotazione di un titolo ogni 15 minuti!)

Il passaggio obbligato tra il sistema tradizionale e quello impostato su Internet è una sostanziale revisione culturale, oltre che tecnologica, del modo di comunicare.

Anche la sicurezza rappresenta un problema culturale, poiché, molto spesso, se c'è da tagliare alcune spese, le prime sono quelle informatiche, in particolare quelle per la sicurezza; oggi questa mentalità sta cambiando, poiché ci si rende conto che la mancanza di sicurezza può provocare molti più danni economici di quanto si possa spendere per instaurarla.

4. Analisi, dati, previsioni¹⁷³

¹⁷³ A.A.V.V. a cura di Emilio Tosi, I prolemi giuridici di Internet, diritto dell'Informatica - collana diretta da Guido Alpa, Milano, Giuffrè, 1999; Anti-phishing Working Group (<http://www.antiphishing.org>); Anti-Phishing Italia (<http://www.anti-phishing.it>); Governo Italiano

Il 2004 verrà ricordato come l'anno del phishing, cioè un anno in cui è nato un "nuovo" crimine informatico.

Questo è un fenomeno preoccupante, i messaggi di e-mail phishing rilevati nei primi mesi del 2005 confermano un trend di crescita contenuto, ma costante e pertanto da non sottovalutare.

Invece, particolarmente significativi i casi registrati tra agosto 2005 e agosto 2006, dove le segnalazioni di questo tipo di attacco hanno raggiunto dei picchi decisamente preoccupanti.

Infatti, il vero record si è verificato con 28.571 siti "fasulli" identificati nel giugno 2006, come si può analizzare dal grafico sottostante.



174

Ma non è solo una questione di numeri. Secondo gli esperti, uno dei problemi più evidenti è che gli attacchi stanno diventando via via sempre più complessi, sfruttando modalità sempre più difficili da individuare.

Infatti, col proseguire di tale fenomeno, le tecniche si sono fatte sempre più raffinate e si sono aggiunti stratagemmi da "social engineering". (cercare di indurre un utente a fare qualcosa utilizzando un metodo non tecnologico, ma "psicologico")

Infatti, due sono le nuove tecniche adottate dai phisher: la prima è rappresentata dal "Voip", grazie alla crescente diffusione dei servizi voce su Internet a basso costo e alla relativa impreparazione degli enti su questo argomento, i responsabili degli abusi iniziano a chiamare le vittime designate, invece di inviare loro un messaggio via posta elettronica.

I destinatari possono così ascoltare un messaggio che li avvisa di un problema relativo al loro conto bancario e vengono invitati a chiamare un certo numero per risolvere il problema.

Chiamato il numero, passano attraverso il sistema vocale che chiede di inserire il numero di carta di credito; la seconda si concretizza in un attacco in

(<http://www.governo.it/index.asp>); Criminologia – Rivista Internet di Teoria e Scienze Criminali - (<http://www.criminologia.it>); Rivista Telematica Full-text di Criminologia Clinica e Psicologica Investigativa - (<http://www.criminologia.org>); Polizia di Stato – Polizia Postale (<http://www.poliziadistato.it>).

¹⁷⁴ Grafico estratto dal sito <http://www.antiphishing.org>

tempo reale e il phisher riesce a neutralizzare la sicurezza aggiuntiva fornita dal password-token che sincronizzato con il server della banca forniscono una nuova password ad intervalli regolari.

Alcuni phishers sono, infatti, riusciti a creare “pagine-trappola” dove gli utenti ignari vengono spinti ad inserire tutti i dati necessari all'autenticazione bancaria: numero di conto, password personale e codice numerico generato dal token.

Attraverso un sofisticato script, il phisher si connette in tempo reale alla banca della vittima e sfrutta il codice generato dal token prima che diventi inefficace.

In questa finestra temporale, che può durare anche solo pochi secondi, i truffatori sarebbero in grado di trasferire fondi o effettuare qualsiasi altro tipo di operazione bancaria.

Pertanto, le previsioni per il futuro non sono buone, poichè sono previste frodi via e-mail più personalistiche e proprio in questa ottica è bene cominciare a pensare alle reazioni non solo di carattere normativo (sempre più lente ad arrivare), ma soprattutto di carattere tecnologico.

Una truffa informatica permette agli ideatori di capire, attraverso l'e-mail, i dati di accesso personali alla propria banca online.

In Italia finalmente la prima condanna per phishing:

Due truffatori avevano predisposto una rete di conti bancari, per riciclare all'estero il denaro di numerose frodi.

I due appartenevano ad una sofisticata organizzazione criminale operante in Europa.

Nel luglio 2006, il tribunale di Milano, per la prima volta in Italia ha condannato per phishing i due truffatori rispettivamente a quattro anni e quattro anni e sei mesi oltre una sanzione di 4000 euro.

Dalla sentenza si apprende il loro modus operandi: con documenti falsi e clonati creavano società “fasulle” con l'obiettivo di aprire il maggior numero di conti bancari intestati alle stesse società, inoltre contattavano diversi titolari di conti in Italia per coinvolgerli nell'attività di riciclaggio di denaro.

Gli intestatari, mettendo a disposizione i loro conti, guadagnavano in percentuale sul flusso di denaro che transitava, ma facilitavano in realtà la trasmissione del denaro all'estero, attraverso bonifici su conti esteri.

Disegno criminoso scoperto dalla guardia di finanza in collaborazione con la direzione centrale tutela aziendale di poste italiane.

Le indagini proseguono sul fronte del phishing e del riciclaggio, indagati circa 80 intestatari dei conti.

Persone più o meno consapevoli delle loro azioni, che dovranno essere valutate da un magistrato caso per caso.

Questi comportamenti criminosi sembrano essere in Italia solo i primi di una possibile lunga serie.

Fino ad ora, nel nostro paese la situazione è stata ancora controllabile, infatti in seguito ad un'indagine compiuta su un campione significativo di utenti avente ad oggetto la nota insidia telematica, è emerso che il 36% degli

utenti avrebbe subito attacchi di phishing, e fra questi, il 5% si sia recato presso i link indicati nell'e-mail.

Situazione ben differente se si osservano indagini compiute a livello mondiale, infatti secondo l'Anti-Phishing Working Group (APWG), i siti di phishing tradizionali crescono, ogni mese, del 50%.

Proprio per questo motivo Microsoft, e-Bay e Visa hanno deciso di dar vita al "Phishing Report Network" una sorta di database che raccoglie le informazioni utili per identificare l'e-mail "truffaldine" che arrivano agli utenti di tutto il mondo e che consentirà di stilare una lista nera dei siti del phishing a cui sono stati attribuiti molti tentativi di truffa.

Infatti, la polizia postale, quale organo di controllo, ha inviato una circolare all'Associazione bancaria italiana (ABI) invitando le banche ad avvertire i propri clienti di non digitare i codici personali nel caso dovessero ricevere questo tipo di e-mail.

L'ABI ha prontamente riunito in un decalogo le regole utili per difendersi dal phishing:

- “1. Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali;
2. è possibile riconoscere le truffe via e-mail con qualche piccola attenzione: generalmente queste e-mail non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati; fanno uso di toni intimidatori; non riportano una data di scadenza per l'invio delle informazioni;
3. nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca tramite;
4. non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale;
5. diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;
6. quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con .https://. E non con .http://. E nella parte in basso a destra della pagina è presente un lucchetto;
7. diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking;
8. controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito;
9. le aziende produttrici dei browser rendono periodicamente disponibili online e scaricabili gratuitamente degli aggiornamenti (le cosiddette patch) che incrementano la sicurezza di questi programmi;

10. Internet è un po' come il mondo reale: come non daresti a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo.

In caso di dubbio, rivolgetevi alla vostra banca”.

Infine, come si è potuto apprendere da un'analisi minuziosa di tale problematica per prevenire, arginare e limitare la diffusione di codesto reato bisogna adottare molteplici soluzioni per garantire la sicurezza dei sistemi informatici, nonché il rispetto delle regole.

Sicuramente è molto difficile frenare queste condotte criminose, perché nell'era di internet tutto avviene ad una velocità estrema. I punti cardini su cui soffermarsi per cercare di risolvere in parte il reato di phishing sono, in primis, una esaustiva e approfondita informazione a tutti gli utenti di internet coordinata con l'utilizzo di software sempre più precisi ed aggiornati, nonché l'emanazione e l'applicazione di norme adeguate.

Il crimine informatico, comunque, rimane, a tutt'oggi, un problema da affrontare e da superare che riguarda proprio la disciplina e le regole che devono e dovrebbero regolamentare Internet e i sistemi informatici.

Infine, analizzando i fatti si capisce che l'evoluzione dei sistemi informatici e di Internet è stata talmente veloce che il diritto è rimasto indietro: si pensi solamente all'infinità di reati che si possono compiere sul web e che non trovano una valida regolamentazione secondo diritto.

CAPITOLO X

DANILO BACCI

ASPETTI LEGALI PER LA PUBBLICAZIONE DI SITI E-COMMERCE E CASI DI STUDIO

SOMMARIO: 1. Considerazioni introduttive e definizioni. – 1.1. Condizioni e presupposti amministrativi per l'avvio dell'attività di commercio elettronico. – 1.2. Sanzioni e partita IVA nel sito web. – 1.3. Disciplina del commercio elettronico. – 1.4. Contratto concluso dai consumatori e Codice del Consumo. 1.5. Disposizioni sulla riservatezza e Codice della Privacy. – 2. Autodisciplina e conciliazione on line. 3. Casi studio.

1. Considerazioni introduttive e definizioni.

Questo elaborato compendia e ordina in modo sistematico gli aspetti legali attinenti ai siti che svolgono attività di commercio elettronico. Spesso gli operatori del web (agenzie web, webmaster) nello sviluppare siti di commercio online, disattendono la normativa di riferimento causando problematiche di natura legale al titolare dell'attività imprenditoriale e generando incertezze all'utente finale che non è tutelato nell'acquisto. Attraverso una ricerca superficiale nella rete è possibile notare che la maggior parte dei siti che si trovano nel web non vengono adeguate alla normativa di settore (vedi capitolo.3, casi studio) e quindi soggetti a sanzioni.

Da considerare poi, che l'utente che fa acquisti in internet acquisisce lo status di *consumatore*¹⁷⁵, facendo scaturire dei diritti in capo esso e di conseguenza dei doveri al gestore on line. Un esempio chiarificante è quello delle informazioni obbligatorie da inserire nel sito, la quale mancanza, fa spostare il termine per l'esercizio del diritto di recesso da parte del consumatore da dieci giorni ai novanta giorni (art. 65 comma 3, del D.lgs. n. 206/2005 "Codice del consumo") e la disposizione si applica "*anche nel caso in cui il professionista fornisca una informazione incompleta o errata che non consenta il corretto esercizio del diritto di recesso*" (art. 65 comma 4, del D.lgs. n. 206/2005). Oppure, in caso di controversia (non arriva la merce già pagata o se una volta arrivata non corrisponde a quanto è stato ordinato o dovesse essere difettosa), il procedimento giudiziale si svolgerà presso il domicilio o la residenza del consumatore e non in quello del professionista (competenza territoriale inderogabile), per cui qualsiasi clausola inserita nelle condizioni generali del contratto sulla derogabilità della competenza territoriale (es. presso il domicilio del professionista) è da considerare inefficace (art. 79, "Codice del consumo"). Una soluzione alla inderogabilità

¹⁷⁵ Consumatore è qualsiasi persona fisica che agisca con finalità non riferibili all'attività commerciale, imprenditoriale o professionale eventualmente svolta (art. 3 lett. e, D.Lgs. 70/2003).

della competenza territoriale è disciplinato dal codice del consumo, attraverso una composizione extragiudiziale¹⁷⁶ delle controversie da svolgersi via internet ma al consumatore è data sempre la possibilità di adire il giudice competente qualunque sia l'esito della procedura extragiudiziale (art. 141 comma 5, "Codice del consumo"). Il vantaggio è un risparmio economico per le parti che non devono iniziare nessun procedimento ordinario e soprattutto restringe il tempo della soluzione della stessa controversia.

Altra questione è stabilire rapporto di fiducia del consumatore con il professionista che svolge l'attività di commercio elettronico. Questo è possibile con i codici di autodisciplina (vedi capitolo 2) attraverso i quali il sito deve avere quelle caratteristiche sia tecniche che legali che garantiscono sicurezza nella transazione.

Occorre definire il "commercio elettronico" ai fini delle disposizioni contenute nella normativa applicabile¹⁷⁷. Una prima indicazione per tale individuazione ci viene fornita dalla Commissione UE che, nella Comunicazione "*Un'iniziativa europea in materia di commercio elettronico*"¹⁷⁸, definisce il "commercio elettronico" come "*lo svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica; la distribuzione on-line di contenuti digitali; l'effettuazione per via elettronica di operazioni finanziarie e di borsa; gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo delle Pubbliche Amministrazioni*".

La definizione offre un primo significativo dato: il commercio elettronico non è solo quello relativo agli scambi realizzati tra computer collegati in una rete telematica (come Internet), ma a tutte le fattispecie che implicano l'adozione di strumentazioni elettroniche, indipendentemente dalle modalità e dalle procedure seguite, si pensi alle televendite in radiodiffusione, alle applicazioni su reti "proprietarie" pubbliche o private, nonché alle c.d. offerte off-line, per es. tramite cataloghi su CD-Rom, ecc..

Un'altra indicazione che si può ravvisare dall'approccio descrittivo del legislatore comunitario consiste nel fatto che il commercio elettronico non si esaurisce nello strumento utile per il contatto tra fornitore e compratore, ma si estende a tutte le fasi della distribuzione (eccettuata la consegna che, se si tratta di beni materiali, avverrà tramite i consueti canali): dalla ricerca del potenziale compratore, alla fase della trattativa e negoziazione, alla stipulazione del contratto, al pagamento dei prodotti o servizi acquistati. Il legislatore comunitario¹⁷⁹ inserisce il commercio elettronico nell'alveo dei "*servizi della società dell'informazione*"¹⁸⁰, intendendosi¹⁸¹ per tali "*qualsiasi*

¹⁷⁶ Art. 19, D.Lgs. 70/2003 (Composizione delle controversie).

¹⁷⁷ <http://www.indisunioncamere.it/commercio/guida.htm>

¹⁷⁸ COM/15/4/1997 n.157 - Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni.

¹⁷⁹ Direttiva comunitaria n. 2000/31/CE, dell'8 giugno 2000

¹⁸⁰ **Società dell'informazione:** Nuovo modello di organizzazione delle attività umane basata sulla gestione elettronica delle informazioni e sulla trasmissione delle stesse informazioni attraverso reti di

servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, cioè della persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, anche per ricercare o rendere accessibili delle informazioni".

Molto importante poi, la rilevanza che il legislatore ha dato al documento informatico¹⁸² e con il D.P.R. n. 513/97¹⁸³ attribuendo validità e rilevanza ai documenti informatici, costituendo pertanto la base per la contrattazione su Internet, superando i dubbi e le difficoltà di un riconoscimento ai contratti digitali della stessa tutela che l'ordinamento appresta al documento cartaceo tradizionale.

1.2 Condizioni e presupposti amministrativi per l'avvio dell'attività di commercio elettronico

Nel commercio elettronico occorre verificare se esistono le autorizzazioni per i soggetti che intendono vendere su Internet. Prima di tutto va fatta distinzione di chi opera l'attività economica, perché da questa distinzione scaturisce l'applicabilità¹⁸⁴ del D.Lgs 114/1998¹⁸⁵. Possiamo identificare tre grandi categorie:

- **B2B (Business to Business)**

Indica generalmente i rapporti tra aziende nel mercato dei prodotti industriali. Quest'ultimo si caratterizza per il fatto che acquirente e venditore perseguono gli stessi obiettivi e hanno simili configurazioni organizzativo -decisionali.

- **B2C (Business to Consumer)**

telecomunicazione sempre più estese e capillari, In sostanza si tratta di un modello che si regge sulla gestione elettronica delle informazioni codificate in entità immateriali chiamate bit, abbreviazione dell'inglese "*binary digit*" (cifra binaria): ossia "0" o "1" le due cifre usate nella numerazione binaria che è alla base del linguaggio dei computer, e sulla trasmissione delle stesse informazioni attraverso reti di telecomunicazione sempre più estese e capillari (Glossario della Società dell'Informazione - Università di Pisa, Dipartimento di Informatica).

¹⁸¹ direttiva 98/34/CE del 22 giugno 1998, come modificata dalla direttiva 98/48/CE del 20 luglio 1998

¹⁸² Art. 15 della legge 15 marzo 1997, n. 59 stabilisce che "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*". Questa disposizione conferma il principio generale della validità del documento informatico.

¹⁸³ Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59

¹⁸⁴ Art. 61 codice del Consumo, Decreto Legislativo 6 settembre 2005, n. 206 - "Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229".

¹⁸⁵ D.Lgs. 114 del 31 marzo 1998, "*Riforma della disciplina relativa al settore commercio*", a norma dell'articolo 4, comma 4, della legge 15 marzo 1997, n. 59

Indica l'insieme delle transazioni commerciali di beni e servizi tra imprese e consumatori finali. E' l'azienda a determinare il prezzo dell'oggetto o del servizio oggetto della transazione.

▪ G2C (Government to Citizens)

Si indica per G2C quelle attività oggetto di transazione erogate dal mondo governativo nei confronti del cittadino.

L'art. 4 del D.Lgs. n. 114/98 distingue:

▪ *“commercio all'ingrosso” (B2B) si intende “l'attività svolta da chiunque professionalmente acquista merci in nome e per conto proprio e le rivende ad altri commercianti all'ingrosso o al dettaglio, o ad utilizzatori professionali, o ad altri utilizzatori in grande” (lett.a).*

▪ *“commercio al dettaglio” (B2C) si intende, invece, “l'attività svolta da chiunque professionalmente acquista merci in nome e per conto proprio e le rivende, su aree private in sede fissa o mediante altre forme di distribuzione, direttamente al consumatore finale” (lett.b).*

Nella seconda parte sempre dell'art. 4 indica l'ambito in cui non va applicata la normativa:

- a) agli artigiani, per la vendita nei locali di produzione o nei locali a questi adiacenti dei beni di produzione propria. L'artigianato, a differenza del commerciante, non acquista merci per rivenderle ma vende i beni che produce;
- b) alle associazioni dei produttori ortofrutticoli;
- c) ai titolari di rivendite di generi di monopolio, qualora vendano esclusivamente tali generi;
- d) ai produttori agricoli, singoli o associati, che esercitino attività di vendita di prodotti agricoli nei limiti stabiliti dalla normativa vigente;
- e) alle vendite di carburanti per uso autotrazione, compresi i lubrificanti, nonché di oli minerali;
- f) ai pescatori e alle cooperative di pescatori, nonché ai cacciatori, singoli o associati che vendano al pubblico, al dettaglio la cacciagione e i prodotti ittici provenienti esclusivamente dall'esercizio della loro attività;
- g) a chi venda o esponga per la vendita le proprie opere d'arte, nonché quelle dell'ingegno a carattere creativo, comprese le proprie pubblicazioni di natura scientifica o informativa;
- h) all'attività di vendita effettuata nelle fiere campionarie e nelle mostre di prodotti, purché riguardi le sole merci oggetto delle manifestazioni e non si protragga oltre il periodo di svolgimento di queste ultime;
- i) ai farmacisti che vendano esclusivamente prodotti farmaceutici, specialità medicinali, dispositivi medici e presidi medico-chirurgici;
- j) alla vendita di beni del fallimento;

k) gli enti pubblici o alle persone giuridiche private partecipate dallo Stato o da enti territoriali che vendano pubblicazioni od altro materiale informativo, concernenti l'oggetto della loro attività.

Da quanto detto si traggono i seguenti caratteri comuni:

- a) lo svolgimento dell'attività di commercio deve essere professionale ossia non occasionale¹⁸⁶;
- b) il commercio prevede l'acquisto di prodotti (e/o di servizi)¹⁸⁷.
- c) l'acquisto deve avvenire in nome e per conto proprio;
- d) l'acquisto è finalizzato alla successiva rivendita.

Alla luce della lettura dell'art. 3 lett. b (tutela di informazione per il consumatore), trova giustificazione il Titolo VI del D.Lgs. n. 114/98 (Forme speciali di vendita al dettaglio) che detta regole di comunicazioni più rigorose per B2C rispetto al B2B, poiché nel primo caso le parti non sono posti sullo stesso piano paritetico in cui la parte più debole, il consumatore, deve avere una maggior tutela. In particolare l'art 18 "*Vendita per corrispondenza, televisione o altri sistemi di comunicazione*" che, nel compendiare una serie di tipologie di vendite al dettaglio a distanza e, più esattamente, quelle per corrispondenza e quelle televisive, si riferisce anche a tutte quelle effettuate mediante altri sistemi di comunicazione, quindi anche le vendite elettroniche.

Le regole previste dalla indicata disposizione sono:

- a) comunicazione al Comune nel quale l'operatore ha la residenza, se persona fisica, o la sede legale se società, con la quale dichiara la sussistenza dei requisiti di cui all'art. 5 del decreto, nonché il settore merceologico di attività: alimentare, non alimentare, ovvero entrambi;
- b) la comunicazione deve essere effettuata – in attesa della pubblicazione dell'apposita modulistica da parte del Ministero dell'Industria – tramite il modello COM 1¹⁸⁸, ovvero tramite comunicazione che contenga gli stessi elementi;
- c) l'attività può essere esercitata solo decorsi 30 giorni dal ricevimento della comunicazione da parte del Comune;
- d) è ammesso l'invio di prodotti al consumatore solo se non vi siano vincoli a suo carico, a meno che l'invio non sia stato da questi sollecitato mediante specifica richiesta in tal senso;
- e) Le operazioni di vendita all'asta realizzate per mezzo della televisione o di altri sistemi di comunicazione sono vietate;

¹⁸⁶ Da escludersi dunque i casi di C2C, es. la vendita tra consumatori che avvengono sui siti come ebay (www.ebay.it)

¹⁸⁷ La forma giuridica sarà allora il contratto di compravendita (art. 1470 ss., c.c.) ovvero, nel caso della vendita di giornali e riviste, il contratto estimatorio (art. 1556-1558 c.c.), che è stato dalla giurisprudenza assimilato alla vendita, per le peculiari esigenze della distribuzione di questi prodotti

¹⁸⁸ Pubblicato sulla G.U., serie generale, n. 94 del 23 aprile 1999, nonché sul sito www.attivitaproductive.gov.it, www.unioncamere.it e www.infocamere.it

Il modello COM 1, riguarda la comunicazione per l'apertura, il subingresso, le variazioni (ossia, trasferimento di sede, ampliamento della superficie e la variazione del settore merceologico), nonché la cessazione dell'attività degli esercizi di vicinato e, quindi, non specificamente, l'attivazione del commercio elettronico di cui al sopracitato art. 18. Ne consegue che dovranno essere compilati solo i riquadri compatibili. Le indicazioni necessarie possono essere comunicate al Comune (e poi al Registro delle imprese della Camera di commercio).

Si faceva riferimento al fatto che questo articolo si applica unicamente ai soggetti che esercitano commercio al dettaglio, come risulta dal suo inserimento nel Titolo VI del decreto, dedicato alle forme speciali di vendita al dettaglio, donde si esclude la sua applicabilità alle forme di vendita all'ingrosso effettuate in Rete (B2B).

Ne consegue che, per poter effettuare tali vendite su Internet, i grossisti¹⁸⁹ sono tenuti, unicamente, al possesso dei requisiti soggettivi previsti dall'art. 5 (Requisiti di accesso all'attività) del decreto e, in particolare, di quelli professionali se il commercio riguardi prodotti appartenenti al settore merceologico alimentare. Per il problema della vendita all'ingrosso¹⁹⁰ su Internet l'art. 26, comma 2 del D.Lgs. n. 114/98 proibisce l'esercizio congiunto del commercio all'ingrosso e al dettaglio nello stesso locale, risolve la questione della promiscuità richiedendo all'operatore che voglia svolgere sia l'attività di ingrosso che di dettaglio on line tramite un unico sito di *“.. destinare aree del sito distinte per l'attività all'ingrosso e al dettaglio: in tal modo, infatti, il potenziale acquirente è messo in condizione di individuare chiaramente le zone del sito destinate alle due tipologie di attività”*.

In questo modo, il dettagliante/grossista potrà agevolmente distinguere le modalità di contrattazione con i propri clienti, poste le diverse regole di salvaguardia disposte nei confronti dei consumatori e non anche nei soggetti compratori che non rivestano questo status.

1.2.1 Sanzioni

L'art. 22 del decreto stabilisce che *“chiunque violi le disposizioni di cui agli articoli 5, 7, 8, 9, 16, 17, 18 e 19 del presente decreto è punito con la sanzione amministrativa del pagamento di una somma da lire 5.000.000 a lire 30.000.000”*. E nel secondo comma che *“in caso di particolare gravità o di recidiva il sindaco può inoltre disporre la sospensione della attività di vendita per un periodo non superiore a venti giorni. La recidiva si verifica qualora sia stata commessa la stessa violazione per due volte in un anno, anche se si è proceduto al pagamento della sanzione mediante oblazione”*.

¹⁸⁹ Circolare n.3487/C 01/06/2000 Ministero dell'Industria, del Commercio e dell'Artigianato sul decreto legislativo 31 marzo 1998, n. 114. Disciplina della vendita di beni tramite mezzo elettronico. Commercio elettronico.

¹⁹⁰ Art. 64 comma 1 codice del consumo

1.2.2 Indicazione del numero di partita Iva nel sito web

Quesito: il numero di partita Iva, attribuito dagli uffici dell'Agenzia a quanti intraprendono l'esercizio di impresa, arte o professione nel territorio dello Stato, deve o meno essere indicato nella home-page del sito web anche nel caso in cui il sito venga utilizzato per scopi meramente propagandistici e pubblicitari, senza il compimento di attività di commercio elettronico?

Questo è stato il quesito posto all'Agenzia delle Entrate¹⁹¹ in riferimento al D.P.R. 633/1972¹⁹² in particolare l'articolo 35¹⁹³, comma 1, che dispone che " ... *L'ufficio attribuisce al contribuente un numero di partita I.V.A. che resterà invariato anche nelle ipotesi di variazioni di domicilio fiscale fino al momento della cessazione dell'attività e che deve essere indicato nelle dichiarazioni, nella home-page dell'eventuale sito web e in ogni altro documento ove richiesto ...*" e il secondo comma del medesimo articolo lett.e dispone successivamente, "*dalla dichiarazione di inizio attività devono risultare per i soggetti che svolgono attività di commercio elettronico, l'indirizzo del sito web ed i dati identificativi dell'internet service provider; ...*" Da un'interpretazione sistematica delle disposizioni in commento emerge che l'adempimento previsto all'articolo 35, comma 1, ha natura e finalità differenti rispetto a quello contenuto nel comma 2, lettera e), limitato ai soli soggetti che effettuano attività di commercio elettronico.

L'obbligo di indicazione del numero di partita Iva nel sito web rileva per tutti i soggetti passivi Iva, a prescindere dalle concrete modalità di esercizio dell'attività. Di conseguenza, quando un soggetto Iva dispone di un sito web relativo all'attività esercitata, quando anche utilizzato solamente per scopi pubblicitari, lo stesso è tenuto ad indicare il numero di partita Iva, come chiaramente disposto dall'articolo 35, comma 1.

L'articolo 35, comma 2, lettera e), concerne, invece, il contenuto della dichiarazione di inizio attività, la cui presentazione è un adempimento che precede l'attribuzione della partita Iva ed è finalizzato, fra l'altro, all'acquisizione da parte dell'Amministrazione finanziaria delle informazioni inerenti all'attività da esercitare.

1.3 Disciplina del commercio elettronico

D.Lgs. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico)

¹⁹¹ Agenzia Entrate, risoluzione 16.05.2006 n° 60 - www.agenziaentrate.it

¹⁹² D.P.R. 26 ottobre 1972, n. 633, Istituzione e disciplina dell'imposta sul valore aggiunto - GU n. 292 del 11-11-1972

¹⁹³ Modificato dall'articolo 2, comma 1, del decreto del Presidente della Repubblica 5 ottobre 2001, n. 404 (in vigore dal 1 dicembre 2001)

In attuazione della direttiva 2000/31/CE¹⁹⁴, il D.Lgs. 70/2003 va disciplinare e promuovere la libera circolazione dei servizi della società dell'informazione e in particolare il commercio elettronico (art. 1 "Finalità"). Le norme del presente decreto si applicano al prestatore¹⁹⁵ dei servizi della società dell'informazione stabilito sul territorio italiano, ma questo concetto di stabilimento *"non va riferito al luogo in cui si trovano i mezzi tecnici e le tecnologie necessarie ad effettuare la prestazione del servizio: ciò implica che la sede del prestatore di servizi oggetto della direttiva prescinde dall'ubicazione dei server o dei siti web utilizzati dal medesimo per la prestazione di tali servizi"*¹⁹⁶. Questo decreto disciplina le seguenti categorie: B2B, B2C ma è esclusa quella del C2C¹⁹⁷.

L'art. 6 sancisce che *"l'accesso all'attività di un prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente"*. Ad una prima lettura sembrerebbe che contrasti con D.Lgs. n. 114/98¹⁹⁸ che detta le condizioni per l'avvio delle attività commerciali anche per quelle online. La ratio del D.Lgs. n. 114/98 è quello di verificare se l'attività che si vuol mettere sul mercato sia conforme e non violi i principi che sono già applicabili alle attività commerciali non online, quindi per una questione di uniformità e tutela del consumatore, è preferibile la sua applicazione. Per rafforzare quanto detto, il codice del consumo (vedi paragrafo 1.4, Contratto concluso dai consumatori - Codice del Consumo) nell'art. 61 rinvia per i contratti a distanza l'applicazione della disposizione dell'art. 18 del D.Lgs. n. 114/98 e altresì nell'art. 146 del codice del consumo, che indica le norme che sono abrogate, richiama il D.Lgs. n. 114/98 solo per indicare l'inefficacia dell'art. 18 comma 7 e dell'art. 19 comma 9, mantenendo, quindi, la validità nella sua integrità il decreto.

1.3.1 Informazioni generali obbligatorie

Dal sito deve esser facilmente accessibile per il consumatore, in modo diretto e permanente le seguenti informazioni obbligatorie (art. 7):

- a) il nome, la denominazione o la ragione sociale;
- b) il domicilio o la sede legale;
- c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;

¹⁹⁴ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("*Direttiva sul commercio elettronico*").

¹⁹⁵ Prestatore: è la persona fisica o giuridica che presta un servizio della società dell'informazione (art. 3 lett. b, D.Lgs. 70/2003).

¹⁹⁶ Dalla relazione al D.Lgs. 70/2003

¹⁹⁷ Art. 4 lett. f (esclude le obbligazioni contrattuali riguardanti i contratti conclusi dai consumatori), che deroga l'art. 3 del medesimo decreto.

¹⁹⁸ Vedi paragrafo 1.2

- d) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese;
- e) gli elementi di individuazione, nonché gli estremi della competente autorità di vigilanza qualora un'attività sia soggetta a concessione, licenza od autorizzazione;
- f) per quanto riguarda le professioni regolamentate:
 - 1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione;
 - 2) il titolo professionale e lo Stato membro in cui è stato rilasciato;
 - 3) il riferimento alle norme professionali e agli eventuali codici di condotta vigenti nello Stato membro di stabilimento e le attività di consultazione dei medesimi;
- g) il numero della partita IVA o altro numero di identificazione considerato equivalente nello Stato membro, qualora il prestatore eserciti un'attività soggetta ad imposta;
- h) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;
- i) l'indicazione delle attività consentite al consumatore e al destinatario del servizio e gli estremi del contratto qualora un'attività sia soggetta ad autorizzazione o l'oggetto della prestazione sia fornito sulla base di un contratto di licenza d'uso.

1.3.2 Comunicazioni commerciali on line

In aggiunta agli obblighi informativi previsti per specifici beni e servizi, le comunicazioni commerciali che costituiscono un servizio della società dell'informazione o ne sono parte integrante, devono contenere, sin dal primo invio, in modo chiaro ed inequivocabile, una specifica informativa, diretta ad evidenziare (art. 8):

- a) che si tratta di comunicazione commerciale;
- b) la persona fisica o giuridica per conto della quale è effettuata la comunicazione commerciale;
- c) che si tratta di un'offerta promozionale come sconti, premi, o omaggi e le relative condizioni di accesso;
- d) che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione.

Le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni (art. 9).

1.3.3 Regolamentazione dei contratti conclusi per via elettronica

Qui di seguito sono elencate categorie di contratti che non possono essere conclusi per via elettronica (art. 11):

- a) contratti che istituiscono o trasferiscono diritti relativi a beni immobili, diversi da quelli in materia di locazione;
- b) contratti che richiedono per legge l'intervento di organi giurisdizionali, pubblici poteri o professioni che implicano l'esercizio di pubblici poteri;
- c) contratti di fideiussione o di garanzie prestate da persone che agiscono a fini che esulano dalle loro attività commerciali, imprenditoriali o professionali;
- d) contratti disciplinati dal diritto di famiglia o di successione.

Il prestatore, salvo diverso accordo tra parti che non siano consumatori, deve fornire in modo chiaro (art. 12), comprensibile ed inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario del servizio, le seguenti informazioni (non è applicabile ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti):

- a) le varie fasi tecniche da seguire per la conclusione del contratto;
- b) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;
- c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore;
- d) gli eventuali codici di condotta cui aderisce e come accedervi per via telematica;
- e) le lingue a disposizione per concludere il contratto oltre all'italiano;
- f) l'indicazione degli strumenti di composizione delle controversie.

Le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica (art. 13 comma 1).

Salvo differente accordo tra parti diverse dai consumatori, il prestatore deve, senza ingiustificato ritardo e per via telematica, accusare ricevuta dell'ordine del destinatario contenente un riepilogo delle condizioni generali e particolari applicabili al contratto, le informazioni relative alle caratteristiche essenziali del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili (art. 13 comma 2).

L'ordine e la ricevuta si considerano pervenuti quando le parti alle quali sono indirizzati hanno la possibilità di accedervi (art. 13 comma 3).

Anche in questi casi non si applicano ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti (art. 13 comma 4).

1.3.4 Sanzioni

L'art. 21 del decreto stabilisce che *“salvo che il fatto costituisca reato, le violazioni di cui agli articoli 7, 8, 9, 10 e 12 sono punite con il pagamento di una sanzione amministrativa pecuniaria da 103 euro a 10.000 euro”*.

Nel secondo comma disciplina in caso di recidiva: *“nei casi di particolare gravità o di recidiva i limiti minimo e massimo della sanzione indicata al comma 1 sono raddoppiati”*.

1.4 Contratto concluso dai consumatori - Codice del Consumo¹⁹⁹

D.Lgs. 206/2005 (Codice del Consumo)

Con il D.Lgs. 206/2005 entra in vigore nell'ordinamento italiano il Codice del Consumo, rappresenta²⁰⁰ il testo fondamentale di riferimento in materia di tutela dei diritti dei consumatori e degli utenti. Per la prima volta, il Codice fa assumere un autonomo rilievo al diritto dei consumatori²⁰¹ nell'ambito dell'ordinamento civile e la sua articolazione si ispira alle teorie sul processo di acquisto. Il Codice riunisce, coordina e semplifica²⁰² le disposizioni normative incentrate intorno alla figura del consumatore, come cittadino conscio dei propri diritti e doveri. A tale scopo l'art. 146 abroga quelle discipline che sono regolate dal codice, in particolare per il commercio elettronico²⁰³:

- il decreto legislativo 15 gennaio 1992, n. 50, recante attuazione della direttiva 85/577/CEE, in materia di contratti negoziati fuori dei locali commerciali (art. 146 lett. c);
- il decreto legislativo 22 maggio 1999, n. 185, recante attuazione della direttiva 97/7/CE, relativa alla protezione dei consumatori in materia di contratti a distanza (art. 146 lett. h);
- il comma 9 dell'articolo 19 del decreto legislativo 31 marzo 1998, n. 114 (art. 146 lett. q);
- il comma 7 dell'articolo 18 del decreto legislativo 31 marzo 1998, n. 114 (art. 146 lett. p).

¹⁹⁹ Decreto Legislativo 6 settembre 2005, n. 206, Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229

²⁰⁰ http://www.governo.it/GovernoInforma/Dossier/codice_consumo/index.html

²⁰¹ Art. 2, D.Lgs. 206/2005 (diritti dei consumatori)

²⁰² Art. 3 lett. f “il presente decreto legislativo di riassetto delle disposizioni vigenti in materia di tutela dei consumatori”, D.Lgs. 206/2005

²⁰³ Capo I” PARTICOLARI MODALITÀ DI CONCLUSIONE DEL CONTRATTO” nella Sezione II “Contratti a distanza” del D.Lgs. 206/2005

Rimangono ancora applicabile:

- le disposizioni di cui all'articolo 18 del decreto legislativo 31 marzo 1998, n. 114, recante riforma della disciplina relativa al commercio (art. 61);
- le disposizioni del decreto legislativo 9 aprile 2003, n. 70 (art. 52 comma 5 e art. 68).

Il Codice è orientato a favorire l'informazione del consumatore, a tutelarlo nella fase di raccolta delle informazioni, ad assicurare la correttezza dei processi negoziali e delle forme contrattuali da cui discendono le decisioni di acquisto.

Vengono definiti inoltre in modo chiaro i diritti e gli interessi individuali e collettivi dei consumatori e degli utenti, promuovendone la tutela in sede nazionale e locale, anche in forma collettiva.

1.4.1 Informazioni per il consumatore

Il fornitore deve innanzitutto adempiere ai seguenti due obblighi informativi (art. 52 comma 1):

- 1) sulla schermata finale di conferma dell'ordine del prodotto o di richiesta del servizio devono essere indicati tassativamente i seguenti dati:
 - a) identità del professionista e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del professionista;
 - b) caratteristiche essenziali del bene o del servizio;
 - c) prezzo del bene o del servizio, comprese tutte le tasse e le imposte;
 - d) spese di consegna;
 - e) modalità del pagamento, della consegna del bene o della prestazione del servizio e di ogni altra forma di esecuzione del contratto;
 - f) esistenza del diritto di recesso o di esclusione dello stesso, ai sensi dell'articolo 55, comma 2;
 - g) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;
 - h) costo dell'utilizzo della tecnica di comunicazione a distanza, quando è calcolato su una base diversa dalla tariffa di base;
 - i) durata della validità dell'offerta e del prezzo;
 - j) durata minima del contratto in caso di contratti per la fornitura di prodotti o la prestazione di servizi ad esecuzione continuata o periodica.

- 2) Possibilità per il consumatore di stampare o di operare un download della summenzionata schermata sia prima della conferma mediante pulsante o click del mouse che dopo ed obbligo di chiedere una seconda volta la conferma dell'ordine. La stampa della schermata di conferma serve per dimostrare l'avvenuto ordine (art. 52 comma 2) e contenere (art. 53 comma 1):

- a) un'informazione sulle condizioni e le modalità di esercizio del diritto di recesso (art.64, inclusi i casi di cui all'articolo 65, comma 3);
- b) l'indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;
- c) le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;
- d) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno.

Nel quinto comma dell'art. 52 sottolinea che *“in caso di commercio elettronico gli obblighi informativi dovuti dal professionista vanno integrati con le informazioni previste dall'articolo 12 del decreto legislativo 9 aprile 2003, n. 70”*(vedi paragrafo 1.3.3 Regolamentazione dei contratti conclusi per via elettronica).

1.4.2 Diritto di recesso

Per gli acquisti on-line è previsto un diritto di recesso per il consumatore (artt. 64 e ss), il quale esercita questo diritto senza alcuna penalità e senza specificarne il motivo. Può revocare il proprio ordine entro il termine di dieci giorni lavorativi dalla consegna della merce.

Il consumatore deve esser informato dal venditore sui seguenti aspetti:

- a) modalità esercizio del diritto di recesso o di esclusione dello stesso;
- b) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;
- c) informazione sulle condizioni e le modalità di esercizio del diritto di recesso;
- d) indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;
- e) informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;
- f) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno.

In mancanza di uno di queste informazioni, il termine per l'esercizio del diritto di recesso da parte del consumatore è di sessanta o di novanta giorni (non più dieci) e decorre, per i beni, dal giorno del loro ricevimento da parte del consumatore, per i servizi, dal giorno della conclusione del contratto.

Il termine per l'esercizio del diritto di recesso decorre (art. 65 co 2):

- 1) per i beni, dal giorno del loro ricevimento da parte del consumatore ove siano stati soddisfatti gli obblighi di informazione o dal giorno in cui questi ultimi siano stati soddisfatti, qualora ciò avvenga dopo la conclusione del contratto purché non oltre il termine di tre mesi dalla conclusione stessa(art. 65 comma 2, lett. a);

2) per i servizi, dal giorno della conclusione del contratto o dal giorno in cui siano stati soddisfatti gli obblighi di informazione, qualora ciò avvenga dopo la conclusione del contratto purché non oltre il termine di tre mesi dalla conclusione stessa (art. 65 comma 2, lett. b).

Il diritto di recesso si esercita con l'invio, di una comunicazione scritta alla sede del professionista mediante lettera raccomandata con avviso di ricevimento (art. 64 comma 2). La comunicazione può essere inviata, entro lo stesso termine, anche mediante telegramma, telex, posta elettronica e fax, a condizione che sia confermata mediante lettera raccomandata con avviso di ricevimento entro le quarantotto ore successive; la raccomandata si intende spedita in tempo utile se consegnata all'ufficio postale accettante entro i termini previsti dal codice o dal contratto, ove diversi. L'avviso di ricevimento non è, comunque, condizione essenziale per provare l'esercizio del diritto di recesso²⁰⁴.

La restituzione della merce non comporta automaticamente un valido diritto di recesso dal contratto, a meno che questa possibilità non sia stata prevista espressamente dalle parti nel contratto.

Per i contratti riguardanti la vendita di beni, qualora vi sia stata la consegna della merce, la sostanziale integrità del bene da restituire è condizione essenziale per l'esercizio del diritto di recesso (art. 67 comma 2). La spesa per la riconsegna della merce gravano sul consumatore, se così è stato previsto nel contratto. Altrimenti sono a carico del venditore (art. 67 comma 3).

Il venditore deve, infine, restituire il prezzo pagato dal consumatore entro 30 giorni dal ricevimento della dichiarazione di recesso (art. 67 comma 4). Con la ricezione da parte del professionista della comunicazione mediante lettera raccomandata con avviso di ricevimento, le parti sono sciolte dalle rispettive obbligazioni derivanti dal contratto o dalla proposta contrattuale (art. 66), fatte salve, nell'ipotesi in cui le obbligazioni stesse siano state nel frattempo in tutto o in parte eseguite, le ulteriori obbligazioni.

Il diritto di recesso è escluso dalla legge nei seguenti casi, salvo che il negozio web lo garantisca ugualmente (art. 55):

- per l'acquisto o la vendita di oggetti prodotti appositamente o creati personalmente per il consumatore;
- per beni deperibili o che si modificano velocemente;
- per prodotti audio-video o software sigillati che siano stati aperti dal consumatore;
- per l'acquisto di giornali o riviste;
- per scommesse o lotterie;
- per servizi che, prima della scadenza del termine per esercitare il recesso, siano stati già eseguiti con il consenso del consumatore

²⁰⁴ Art.64 comma 2 codice del consumo

1.4.3 Sanzioni

Nell'art. 62 stabilisce che nel caso in cui il professionista “ *non fornisce l'informazione al consumatore, ovvero ostacola l'esercizio del diritto di recesso ovvero fornisce informazione incompleta o errata o comunque non conforme sul diritto di recesso da parte del consumatore secondo le modalità di cui agli articoli 64 e seguenti, ovvero non rimborsa al consumatore le somme da questi eventualmente pagate, nonché nei casi in cui abbia presentato all'incasso o allo sconto gli effetti cambiari prima che sia trascorso il termine di cui all'articolo 64, è punito con la sanzione amministrativa pecuniaria da euro cinquecentosedici a euro cinquemilacentosessantacinque*”.

Nel secondo comma del medesimo articolo regola i “*casi di particolare gravità o di recidiva, i limiti minimo e massimo della sanzione indicata al comma 1 sono raddoppiati. La recidiva si verifica qualora sia stata commessa la stessa violazione per due volte in un anno, anche se si è proceduto al pagamento della sanzione mediante oblazione*”²⁰⁵

1.5 Disposizioni sulla riservatezza - Codice della Privacy

D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali)

Il cliente che accede nel sito e-commerce per fare acquisti, deve registrarsi, inviando informazioni che lo riguardano, la residenza, dati anagrafici, ecc., tutti dati personali che vengono conservati nel data base del sito. Tutte le operazioni di comunicazione, registrazione, archiviazione, rientrano nella categoria del “*trattamento dei dati personali*” disciplinato dal Codice della Privacy²⁰⁶. Rispetto alla normativa precedente²⁰⁷, ora non è necessario chiedere il consenso del trattamento in quando “*è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato*”²⁰⁸. In un rapporto contrattuale non c'è bisogno del consenso,

²⁰⁵ Nell'art. 62 comma 3: Le sanzioni sono applicate ai sensi della legge 24 novembre 1981, n. 689. Fermo restando quanto previsto in ordine ai poteri di accertamento degli ufficiali e degli agenti di polizia giudiziaria dall'articolo 13 della predetta legge n. 689 del 1981, all'accertamento delle violazioni provvedono, d'ufficio o su denuncia, gli organi di polizia amministrativa. Il rapporto previsto dall'articolo 17 della legge 24 novembre 1981, n. 689, è presentato alla Camera di commercio, industria, artigianato e agricoltura della provincia in cui vi è la residenza o la sede legale del professionista, ovvero, limitatamente alla violazione di cui all'articolo 58, al Garante per la protezione dei dati personali.

²⁰⁶ Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali - pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - si può visionare nel sito: <http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm> - Supplemento Ordinario n. 123

²⁰⁷ Legge 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" - pubblicata nella Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - si può visionare nel sito: <http://www.parlamento.it/parlam/leggi/96675l.htm> - Supplemento Ordinario n. 3

²⁰⁸ Art. 24 lett. b, codice della Privacy

ma della sola informativa, se i dati sono utilizzati per la stretta esecuzione del contratto.

Gli obblighi del professionista è quello di rendere disponibile l'informativa sull'utilizzo dei dati del cliente, in dettaglio (art. 13) l'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto:

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

Quanto riguarda la lett. e, diritti di accesso, disciplinato dall'art. 7 della stessa normativa, l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati personali;
- b) delle finalità e modalità del trattamento;
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

1.5.1 Sanzioni

L'art. 15 stabilisce che “chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050²⁰⁹ del codice civile”. Nel secondo comma amplia la tutela: “il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11²¹⁰”.

Nel caso di omessa o inidonea informativa all'interessato indicato dall'art. 13, si è puniti “*con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore*”.

Nella cessazione (art. 16 lett. b), per qualsiasi causa, di un trattamento i dati sono ceduti ad altro titolare e questi sono destinati ad un trattamento in termini non compatibili agli scopi per i quali i dati sono raccolti si è puniti con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro (art. 162 comma 1).

²⁰⁹ A livello pratico significa che chi tratta i dati, per evitare ogni responsabilità, deve dimostrare di aver adottato “*tutte le misure idonee ad evitare il danno*”. Significa dunque che il titolare dei dati deve dare prova (con l'ausilio anche del Documento Programmatico Sulla Sicurezza) di aver adottato tutte le misure di sicurezza nella miglior versione possibile. Chi omette di adottare le misure minime previste dall'art 33 (misure di sicurezza) è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro (art. 169).

²¹⁰ Art. 11 comma 1: “*I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*”. Nel secondo comma: “*i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*”.

Nel trattamento illecito di dati l'art. 167 comma 1 stabilisce che *“chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129 (elenchi di abbonati), e' punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi”*. Nel secondo comma sempre dell'art. 167 punisce *“chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni”*.

2 Autodisciplina e conciliazione on-line (codice di condotta²¹¹)

2.1 Codice “internet @ minori”

Una piccola frazione del materiale sulla Rete può essere classificato come inappropriato, questa piccola percentuale è altamente visibile e controversa. Ed è per questo che per sviluppare il pieno potenziale educativo di Internet per i minori, queste preoccupazioni devono essere affrontate in maniera efficace²¹². Per tale esigenza nasce il codice internet @ minori, che si pone i seguenti obiettivi e finalità:

- 1) aiutare gli adulti, i minori e le famiglie a un uso corretto e consapevole della rete telematica, tenendo conto delle esigenze del minore;
- 2) predisporre apposite tutele atte a prevenire il pericolo che il minore venga in contatto con contenuti illeciti o dannosi per la sua crescita:
 - a) l'aderente²¹³ deve fornire servizi di navigazione differenziata;
 - b) identificatori di età.
- c) offrire, nel rispetto della normativa nazionale ed internazionale, un accesso paritario e promuovere un accesso sicuro per il minore alle risorse di rete;
- d) tutelare il diritto del minore alla riservatezza ed al corretto trattamento dei propri dati personali;
- e) assicurare, nel rispetto dell'ordinamento vigente, una collaborazione piena alle autorità competenti nella prevenzione, nel contrasto e nella repressione della criminalità informatica ed in particolare nella lotta contro lo sfruttamento della prostituzione, la pornografia ed il turismo sessuale in danno di minori, attuati tramite l'utilizzo della rete telematica;

²¹¹ Codice di condotta: viene definito nell'art.2 lett. f della direttiva 2005/29/CE: *“è un accordo o una normativa che non sia imposta da disposizioni legislative, regolamenti o amministrative di uno Stato membro e che definisce il comportamento dei professionisti che si impegnano a rispettare tale codice in relazione a una o più pratiche commerciali o ad uno o più settori imprenditoriali specifici”*

²¹² Prefazione del codice del Consumo di Lucio Stanca Ministro per l'Innovazione e le Tecnologie

²¹³ Aderente: Il soggetto che svolge attività imprenditoriale su internet, anche a titolo non direttamente oneroso per Clienti ed Utenti, e che aderisce al Codice direttamente o per tramite delle Associazioni firmatarie (art. 1).

- f) agevolare, nel rispetto dell'art. 9 del D.Lgs. n. 70/2003 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, la tutela del minore nei confronti delle informazioni commerciali non sollecitate o che sfruttino la debolezza del minore, ovvero, secondo quanto previsto all'art. 130 del D.Lgs. n. 196/2003, nei confronti delle comunicazioni indesiderate;
- g) diffondere presso gli operatori e le famiglie il contenuto del Codice di autoregolamentazione.

2.2 Codice di Autodisciplina e-Commerce

2.2.1 Introduzione

Istituti di valutazione indipendenti²¹⁴, su richiesta del venditore on-line, valutano se alla base del servizio offerto sussista un rapporto contrattuale rispettoso dei diritti del consumatore e se siano state rispettate soddisfacenti disposizioni di sicurezza. Se l'offerente rispetta tutti i criteri prefissati dall'istituto di valutazione, gli viene rilasciato un attestato e l'autorizzazione di esporre sul proprio sito Internet il marchio di qualità rilasciato dall'istituto stesso (per lo più un emblema grafico).

Poiché i vari istituti adottano criteri e procedimenti differenti per la valutazione, non esiste uno standard generalizzato di qualità. Sono raccomandabili innanzitutto quegli istituti che anche dopo il conferimento del marchio effettuano controlli sul rispetto dei criteri o che danno la possibilità al consumatore di intentare un procedimento di conciliazione vincolante per il venditore virtuale in caso di problemi.

Questi istituti si riservano normalmente la possibilità di ritirare il sigillo di qualità al membro che non abbia rispettato i criteri prefissati o che non si sia attenuto alla decisione arbitrale; esempi di simili marchi di qualità:

- 1) www.progettofiducia.it (Federcomin)
- 2) www.trustedshops.de
- 3) www.guetezeichen.at
- 4) www.euro-label.com

2.3 Codice “Progetto Fiducia” Federcomin

La Federcomin, federazione nazionale di settore di Confindustria che rappresenta le imprese di telecomunicazioni, radiotelevisione e informatica, ha creato il Marchio Fiducia Federcomin con l'obiettivo di migliorare la fiducia di chi acquista on-line.

Federcomin, recependo le indicazioni contenute nella direttiva CE sul commercio elettronico dell'8 giugno 2000 (Dir. 2000/31/CE in GUCE L178 del 17 luglio 2000) che prevede e incoraggia "l'elaborazione di codici di

²¹⁴ <http://www.euroconsumatori.org/16849v21517d21526.html>

condotta a livello comunitario da parte di associazioni e organizzazioni imprenditoriali e professionali" (art.16), ha elaborato un Codice di Comportamento che stabilisce regole di trasparenza, sicurezza e riservatezza al fine di garantire l'affidabilità nelle transazioni economiche on-line. Le imprese che aderiscono al "*Progetto Fiducia Federcomin*" sottoscrivono il Codice di Comportamento ed espongono il Marchio Fiducia Federcomin nelle loro pagine Web dedicate alle attività di e-commerce.

La presenza del Marchio Fiducia Federcomin garantisce che l'impresa si attiene a determinati principi e criteri di trasparenza, sicurezza e riservatezza nel condurre operazioni commerciali on-line. Il Marchio, infatti, assicura che lo scambio elettronico avvenga nel rispetto della privacy, che i dati riportati sul sito siano veritieri e che siano adottate le migliori tecnologie disponibili per la gestione della sicurezza oltre a garantire il rispetto delle regole contrattuali e la corretta applicazione delle procedure per la gestione dei reclami.

Esistono altri fattori che influiscono in modo determinante sullo sviluppo del commercio elettronico, e sono fattori legati ai comportamenti sia delle imprese sia dei consumatori. La grande importanza di questi fattori è stata riconosciuta dalla Commissione UE che, nel piano d'azione e-Europe e nel suo ultimo rapporto "*Go Digital*²¹⁵", parla esplicitamente di un progetto e-confidence per stabilire più fiducia nelle operazioni in Rete.

Ci avviamo quindi ad avere Internet come vero e proprio strumento di lavoro, al pari del fax e del telefono. Enorme quindi è il potenziale di sfruttamento così come le opportunità di business legate alla cosiddetta Net Economy.

2.4 Cert.Impresa.

Un altro servizio simile al "progetto fiducia" che ha lo scopo di creare fiducia nel commercio via web, è "Cert.Impresa" della Infocamere. Le imprese italiane²¹⁶ presenti sul web possono esibire dunque le proprie credenziali ufficiali ai visitatori dei loro siti esponendo sulla home page il logo di Cert.Impresa.

E' un'icona da apporre sulla home page del proprio sito Internet che garantisce la corrispondenza di un determinato indirizzo web ad un'impresa iscritta al Registro delle Imprese. Selezionando sull'icona di Cert.Impresa, i visitatori del sito potranno visualizzare una scheda contenente i dati essenziali dell'impresa cui il sito appartiene²¹⁷:

²¹⁵ Go Digital è una sezione del portale Europeo sulla Società dell'Informazione che si pone l'obiettivo di raccogliere tutte le risorse, le opportunità, le idee e le notizie rilevanti per gli imprenditori e gli attori economici che desiderino approfondire il tema dell'e-business ed evolvere la propria attività valorizzandola attraverso l'innovazione tecnologica e l'uso dell'ICT. Sito di riferimento: http://europa.eu.int/information_society/topics/ebusiness/godigital/index_en.htm

²¹⁶ <http://www.infoimprese.it>

²¹⁷ Per vedere un'esempio funzionante del servizio, collegati ad uno dei siti che hanno già acquisito Cert.Impresa: www.oroditrani.it, www.erretiweb.it

- 1) dati ufficiali, perché provenienti dal Registro delle Imprese
- 2) dati costantemente aggiornati
- 3) dati assolutamente inalterabili e convalidati, mediante l'utilizzo della firma digitale, da InfoCamere, Ente Certificatore riconosciuto dall'AIPA²¹⁸ (Autorità per l'Informatica nella Pubblica Amministrazione).

Cert.Impresa è dedicato a tutte le imprese italiane titolari di un sito web o di un indirizzo elettronico su Internet, regolarmente iscritte nel Registro delle Imprese e in regola con il pagamento del diritto annuale.

E' uno strumento che favorisce la trasparenza dei rapporti su Internet. L'utilità di Cert.Impresa risulta particolarmente evidente per le aziende che svolgono attività di commercio elettronico che, attraverso questo servizio, assicurano la propria clientela sull'identità dell'impresa titolare del sito sul quale stanno acquistando beni e servizi.

Il valore particolare di Cert.Impresa è che, attraverso l'attestato, è possibile avere ogni giorno informazioni aggiornate sull'impresa. Ogni modifica nella denominazione, nell'attività, nei rappresentanti dell'impresa e nei loro poteri sono riprodotti in tempo reale nell'attestato, che va visualizzato ogni volta.

2.3.1 Costi e modalità di richiesta

Il costo del servizio è di Euro 77,00 l'anno pagabile a mezzo carta di credito, bonifico bancario, versamento su c/c postale o presso la Camera di Commercio presso cui è iscritta la sede legale dell'impresa.

Il rinnovo di Cert.Impresa può essere effettuato sempre al costo di € 77,00 e con le stesse modalità di pagamento del primo acquisto. Per ottenere il servizio basta compilare e restituire via fax al call-center di InfoCamere il modulo di richiesta, che può essere scaricato scegliendo uno dei tre formati disponibili.

Il modulo deve essere firmato da una persona avente una carica ufficiale all'interno dell'impresa. La richiesta può essere inoltrata anche alla Camera di Commercio presso cui è iscritta la sede legale dell'impresa.

Il servizio sarà attivato entro 48 ore dal ricevimento della documentazione e rimarrà attivo per i 12 mesi successivi. L'avvenuta attivazione verrà comunicata attraverso l'invio di un messaggio e-mail con le istruzioni per l'inserimento del link al servizio sulla pagina web del richiedente²¹⁹.

²¹⁸ AIPA: In attuazione di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato sul supplemento ordinario n. 123 alla Gazzetta Ufficiale n. 174 del 29 luglio 2003, l'Autorità per l'informatica nella pubblica amministrazione è stata trasformata in Centro nazionale per l'informatica nella pubblica amministrazione. Il nuovo sito del Centro nazionale per l'informatica nella pubblica amministrazione è all'indirizzo <http://www.cnipa.gov.it>

²¹⁹ Per maggiori informazioni, scrivete a: cert.impresa@infocamere.it

2.5 Conciliazione on-line

Per le controversie civili inerenti alle problematiche derivanti dal commercio elettronico (non arriva la merce già pagata o se una volta arrivata non corrisponde a quanto è stato ordinato o dovesse essere difettosa), *“la competenza territoriale inderogabile è del giudice del luogo di residenza o di domicilio del consumatore, se ubicati nel territorio dello Stato²²⁰”*.

Ma è possibile trovare una soluzione alternativa indicata dall'art. 141 del Codice del Consumo, dunque, non sono vessatorie le clausole inserite nei contratti dei consumatori aventi ad oggetto il ricorso ad organi che si conformano alle disposizioni della composizione extragiudiziale della controversia (art. 141 comma 4), ma al consumatore è data sempre la possibilità di adire il giudice competente qualunque sia l'esito della procedura di composizione extragiudiziale (art. 141 comma 5). Nei rapporti tra consumatore e professionista, conviene avviare le procedure di composizione extragiudiziale per la risoluzione delle controversie in materia di consumo, anche in via telematica. Il vantaggio è dato da un procedimento economico e rapido rispetto alla via giudiziaria ordinaria. Nella maggior parte dei casi il procedimento può svolgersi on-line e non è necessaria alcuna comparizione davanti al giudice. I primi modelli²²¹ secondo cui si è sviluppata la risoluzione online delle controversie sono:

1) la negoziazione assistita: due parti si scambiano offerte e controfferte monetarie come durante un'asta, il software blocca la contrattazione quando l'ammontare dei reciproci rilanci ha raggiunto uno scarto del 30% circa. In tali sistemi non è però previsto l'intervento di nessun terzo che aiuti le parti a risolvere la controversia.

2) la conciliazione o mediazione online: le parti dialogano tra loro via e-mail o in chat line alla presenza di un terzo, il conciliatore, che le aiuta a trovare un accordo online. È il modello più fedele all'immagine tradizionale della conciliazione faccia a faccia (ed è il modello di RisolviOnline).

3) l'arbitrato online: le parti affidano la decisione su un caso a un arbitro che non si limita ad aiutarle ma che emette un lodo (una sentenza) sul caso che gli è stato sottoposto. Tutto ciò dopo aver scambiato e inviato via internet la documentazione legata a quel caso. In estrema sintesi, se nella conciliazione ciò che va online è il dialogo tra le parti, nell'arbitrato va online soprattutto lo scambio di documentazione e di memorie arbitrali tra le parti.

Qui di seguito alcuni esempi di conciliazione extragiudiziale:

- **RisolviOnline** della Camera Arbitrale di Milano²²²
- La rete **EEJ-Net**²²³

²²⁰ Art. 63 codice del consumo

²²¹ <http://www.camera-arbitrale.it>

²²² Il sito di riferimento: www.risolvionline.it

2.5.1 Formulario europeo di reclamo

Utile per le parti è il formulario europeo di reclamo²²⁴, elaborato dai servizi della Commissione europea. Esso mira a migliorare il dialogo fra i consumatori e i professionisti e ad aiutarli a raggiungere una composizione amichevole dei problemi che possono incontrare nell'ambito delle loro transazioni.

Esso può essere reperito non soltanto sul sito Internet della Commissione, ma anche presso gli Centri europei dei consumatori EN²²⁵, gli uffici di associazioni di consumatori²²⁶ o altri centri di assistenza e d'informazione per i consumatori²²⁷. Il formulario è disponibile nelle undici lingue ufficiali dell'Unione europea.

Il formulario riguarda:

- 1) i consumatori
- 2) i professionisti
- 3) le associazioni di consumatori
- 4) gli organi extragiudiziari di composizione dei contenziosi riguardanti i consumi.

Il formulario è stato elaborato in maniera da poter orientare il consumatore nella formulazione della sua richiesta. Esso propone una scelta di risposte multiple per aiutare il consumatore a meglio definire i suoi problemi e la sua richiesta, lasciando nel contempo uno spazio sufficiente per consentire agli utilizzatori di aggiungere precisazioni supplementari o descrivere casi particolari non previsti dagli elenchi del formulario.

Nella redazione del formulario, i servizi della Commissione hanno privilegiato nella misura del possibile termini semplici, di uso familiare e comprensibili per i consumatori, invece di utilizzare sistematicamente la terminologia giuridica corrispondente ad ogni situazione distinta. Tuttavia, dato che talvolta è necessario il ricorso a terminologie giuridiche o specifiche, i servizi della Commissione hanno preparato una guida per aiutare gli

²²³ Il sito di riferimento: www.eejnet.org - La Commissione Europea ha elaborato una rete, chiamata EEJ-Net, attraverso la quale al consumatore viene offerta la possibilità di intraprendere un procedimento di conciliazione transfrontaliero.

²²⁴ http://ec.europa.eu/consumers/redress/compl/cons_compl/acce_just03_it.htm

²²⁵ Il Centro Europeo dei Consumatori offre i suoi servizi a tutti i cittadini che incontrano difficoltà nel consumo solo transfrontaliero, ovvero per gli acquisti di beni e servizi da imprese di un altro Stato Membro dell'UE. Il CEC fa anche parte della Rete degli Eurosportelli, istituiti dalla Commissione Europea in quasi tutti gli Stati Membri per assistere i cittadini in caso di problemi nei consumi transfrontalieri. Il Centro Europeo dei Consumatori italiano può esser contattato tramite questo sito: www.ecc-netitalia.it

²²⁶ http://ec.europa.eu/consumers/redress/compl/cons_compl/acce_just03_en_addr.htm

²²⁷ www.euroconsumatori.org

utilizzatori a compilare la parte relativa alla tipologia dei problemi incontrati dal consumatore con alcune domande che il consumatore intende rivolgere al professionista.

Il formulario può essere utilizzato indipendentemente dal valore in gioco e dal tipo di contenzioso riguardante i consumi di cui si tratta. Viene lasciata alle persone interessate la scelta di decidere in quale misura il loro problema possa essere trattato tramite l'utilizzazione del formulario.

Il formulario può essere utilizzato tanto per i contenziosi a livello nazionale quanto per quelli che superano le frontiere nazionali, nel quadro dell'Unione europea. Il sistema di scelte multiple e il fatto che il formulario sia disponibile nelle undici lingue dell'Unione europea, dovrebbe facilitare la questione delle traduzioni nei caso di contenziosi transnazionali nei quali le parti si esprimono in lingue diverse. Il formulario di reclamo europeo non può essere modificato dai suoi utilizzatori.

3 Casi studio.

3.1 www.bancariaeditrice.it (commercio elettronico indiretto)

Descrizione: Bancaria Editrice è stata fondata nel 1974, raccoglie oltre 80 anni di esperienza editoriale dell'ABI Bancaria, le Circolari ABI e l'Annuario delle Banche e finanziarie. Bancaria Editrice è, oggi, la maggiore realtà editoriale italiana specializzata nei temi bancari e finanziari, con 6 riviste, oltre 500 volumi in catalogo, un'attenzione crescente all'editoria elettronica, alla comunicazione e all'organizzazione di convegni ed eventi.

Tipologia del commercio: *Commercio elettronico indiretto*, ha per oggetto le transazioni di beni materiali, ossia di prodotti tangibili dotati di consistenza fisica, che vanno movimentati attraverso i tradizionali canali logistici (corrieri, poste, ferrovia ecc.).

3.1.1 D.Lgs. 70/2003

1) Indicazione del numero di partita Iva nel sito web.

Non presente nella home page ma unicamente nella la sezione "Guida all'acquisto".

2) Informazioni generali obbligatorie.

Per accedere all'informativa bisogna selezionare la sezione "Guida all'acquisto".

oltre al D.Lgs. 70/2003 in vigore il sito fa riferimento al 185/1999 che è stato abrogato e sostituito da codice del consumo. Di seguito vengono verificate l'esistenza delle informazioni generali obbligatorie:

a) il nome, la denominazione o la ragione sociale.

Presente: Bancaria Editrice, Divisione della Società ABIServizi S.p.A., cap Soc. 2.520.000 Euro,

b) il domicilio o la sede legale;

Presente: sede legale in P.zza del Gesù, 49 - 00187 Roma

c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;

Presente: Via della Cordonata, 7 - 00187 Roma, Tel. 06.6767.391/2/3/4/5 Fax 06.6767.397 e-mail servizioclienti@bancariaeditrice.it;

d) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese;

Presente: P. IVA 00988761003, iscritta al registro delle imprese di Roma al n. 3962/74

e) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;

I costi di spedizioni non sono indicati perchè gratuiti. I prezzi dei singoli prodotti sono indicati con iva

3) Comunicazione online

a) che si tratta di comunicazione commerciale

Non è indicato

4) Regolamentazione dei contratti conclusi per via elettronica

a) le varie fasi tecniche da seguire per la conclusione del contratto;

Presente

b) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;

Presente: i contratti telematici conclusi mediante i moduli on-line di cui ai punti precedenti sono conservati, in formato elettronico, in apposita banca dati di ABIServizi S.p.A.; i contraenti potranno richiedere l'invio di una copia telematica di detti contratti tramite e-mail da inviare all'indirizzo info@bancariaeditrice.it

c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore;

Presente: E' possibile durante l'acquisto previa registrazione al sito

d) gli eventuali codici di condotta cui aderisce e come accedervi per via telematica;

Non è presente

e) le lingue a disposizione per concludere il contratto oltre all'italiano;

Presente

f) l'indicazione degli strumenti di composizione delle controversie.

Non indicato

3.1.2 D.Lgs. 206/2005 (Codice del Consumo)

1) Informazioni per il consumatore

Verifica adempimento del fornitore dei due obblighi informativi (art. 52 comma 1):

1) sulla schermata finale di conferma dell'ordine del prodotto o di richiesta del servizio devono essere indicati tassativamente i seguenti dati:

a) identità del professionista e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del professionista;

Presente

b) caratteristiche essenziali del bene o del servizio;

Presente

c) prezzo del bene o del servizio, comprese tutte le tasse e le imposte;

Presente

d) spese di consegna;

E' gratuita

e) modalità del pagamento, della consegna del bene o della prestazione del servizio e di ogni altra forma di esecuzione del contratto;

Presente

f) esistenza del diritto di recesso o di esclusione dello stesso, ai sensi dell'articolo 55, comma 2;

Presente

g) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

Presente

h) costo dell'utilizzo della tecnica di comunicazione a distanza, quando è calcolato su una base diversa dalla tariffa di base;

Non utilizzata

i) durata della validità dell'offerta e del prezzo;

Presente

j) durata minima del contratto in caso di contratti per la fornitura di prodotti o la prestazione di servizi ad esecuzione continuata o periodica.

Presente

2) Possibilità per il consumatore di stampare o di operare un download della summenzionata schermata sia prima della conferma mediante pulsante o click del mouse che dopo ed obbligo di chiedere una seconda volta la conferma

dell'ordine. La stampa della schermata di conferma serve per dimostrare l'avvenuto ordine (art. 52 comma 2) e contenere (art. 53 comma 1):

a) un'informazione sulle condizioni e le modalità di esercizio del diritto di recesso (art.64, inclusi i casi di cui all'articolo 65, comma 3);

Presente

b) l'indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami

Presente

c) le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Presente

d) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno

Presente

e) l'indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;

Presente

f) le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Presente

g) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno

Presente

2) Diritto di recesso

Verifica se il consumatore è informato dal venditore sui seguenti aspetti:

a) modalità esercizio del diritto di recesso o di esclusione dello stesso;

Presente: qualora tu non operi per scopi inerenti la tua attività commerciale, professionale o imprenditoriale, potrai esercitare il diritto di recesso dal contratto relativo ai beni e/o ai servizi richiesti senza alcuna penalità e senza necessità di specificare il motivo, entro 10 gg. lavorativi decorrenti, per i prodotti editoriali (libri e periodici cartacei) dal giorno di ricevimento del bene;

per i servizi telematici (pareri, circolari ed altre riviste on line) e gli altri servizi dal giorno della conclusione del relativo contratto, mediante lettera raccomandata A/R

b) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

Presente

c) c)informazione sulle condizioni e le modalità di esercizio del diritto di recesso;

Presente

d) indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;

Presente

e) informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Presente

f) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno.

Presente

3.1.3 D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali)

Gli obblighi del professionista è quello di rendere disponibile l'informativa sull'utilizzo dei dati del cliente (art. 13). Da quanto si evince dal sito bancariaeditrice.it l'accesso all'informativa su l'utilizzo dei dati personali dal sito e dei diritti del consumatore è visionabile solo nel momento della registrazione, non essendoci un accesso successivo (es. attraverso un link ad una pagina). Verificato:

a) le finalità e le attività del trattamento cui sono destinati i dati;

Presente

b) la natura obbligatoria o facoltativa del conferimento dei dati;

Presente

c) le conseguenze di un eventuale rifiuto di rispondere;

Presente

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

Presente

e) diritto di accesso dell'interessato ai propri dati personali (art. 7);

Presente

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le attività attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Presente

3.1.4 Considerazioni

Il sito bancariaeditrice.it può esser considerato a norma, ma necessita di alcune migliorie:

- nell'accessibilità dell'informativa dei dati personali attraverso una pagina ad hoc;
- consigliabile la presenza della p.iva nella home page;
- inserire nel menu del sito dei nuovi pulsanti per rendere agevole all'utente l'informativa:
 - Pagamenti e garanzia
 - Spedizioni
 - Recesso e reclamo
 - Note legali e Privacy

3.2 www.pdassi.it (commercio elettronico diretto).

Descrizione: Pdassi è il portale per il software dedicato ai palmari basati su Palm OS. Qui è possibile trovare programmi per il palmare: alcuni sono gratuiti, altri possono essere provati in versione dimostrativa ed eventualmente acquistati.

Tipologia del commercio: *Commercio elettronico diretto*, quindi la possibilità di acquistare attraverso la Rete Internet un bene immateriale, ovvero che un bene che non necessita, per essere trasferito, di un supporto fisico, ma che può essere trasferito per via telematica.

3.2.1 D.Lgs. 70/2003.

1) Indicazione del numero di partita Iva nel sito web

Non presente nella home page, neanche in fase di registrazione al sito

2) Informazioni generali obbligatorie

Per accedere all'informativa bisogna selezionare la sezione " Cassa" e successivamente "Spedizioni"

Non è presente il richiamo alla disciplina D.Lgs. 70/2003. Di seguito vengono verificate l'esistenza delle informazioni generali obbligatorie

f) il nome, la denominazione o la ragione sociale:

Presente: Bisogna accedere nella sezione "Copyright", ma ciò risulta fuorviante.

Progetto di envi.con KG Emser Platz 2, D-10719 Berlin Germania, in collaborazione con Handergy s.r.l. via S. Filippo 13, 13900 Biella Italia

g) il domicilio o la sede legale;

Presente: sede operativa Handergy s.r.l. via S. Filippo 13, 13900 Biella Italia

h) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;

Presente: it-support@pdassi.it

i) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese;

Non presente in nessuna parte del sito

j) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;

I costi di spedizioni non sono indicati perchè è un perchè immateriale. I prezzi dei singoli prodotti sono indicati con iva

3) Comunicazione online

b) che si tratta di comunicazione commerciale

E' indicato

4) Regolamentazione dei contratti conclusi per via elettronica

g) le varie fasi tecniche da seguire per la conclusione del contratto;

Presente

h) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;

Non è indicato

i) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore;

Presente: E' possibile durante l'acquisto previa registrazione al sito

j) gli eventuali codici di condotta cui aderisce e come accedervi per via telematica;

Non è presente

k) le lingue a disposizione per concludere il contratto oltre all'italiano;

Presente

l) l'indicazione degli strumenti di composizione delle controversie.

Non indicato

3.2.2 D.Lgs. 206/2005 (Codice del Consumo)

1) Informazioni per il consumatore

Verifica adempimento del fornitore dei due obblighi informativi (art. 52 comma 1):

1) sulla schermata finale di conferma dell'ordine del prodotto o di richiesta del servizio devono essere indicati tassativamente i seguenti dati:

a) identità del professionista e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del professionista;

Presente

b) caratteristiche essenziali del bene o del servizio;

Presente

c) prezzo del bene o del servizio, comprese tutte le tasse e le imposte;

Presente

d) spese di consegna;

E' gratuita perché bene immateriale

e) modalità del pagamento, della consegna del bene o della prestazione del servizio e di ogni altra forma di esecuzione del contratto;

Presente

f) esistenza del diritto di recesso o di esclusione dello stesso, ai sensi dell'articolo 55, comma 2;

Non è indicato

g) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

Non è indicato

h) costo dell'utilizzo della tecnica di comunicazione a distanza, quando è calcolato su una base diversa dalla tariffa di base;

Non utilizzata

i) durata della validità dell'offerta e del prezzo;

Presente

j) durata minima del contratto in caso di contratti per la fornitura di prodotti o la prestazione di servizi ad esecuzione continuata o periodica.

Non è indicato

2) Possibilità per il consumatore di stampare o di operare un download della summenzionata schermata sia prima della conferma mediante pulsante o click del mouse che dopo ed obbligo di chiedere una seconda volta la conferma dell'ordine. La stampa della schermata di conferma serve per dimostrare l'avvenuto ordine (art. 52 comma 2) e contenere (art. 53 comma 1):

a) un'informazione sulle condizioni e le modalità di esercizio del diritto di recesso (art.64, inclusi i casi di cui all'articolo 65, comma 3);

Non è indicato

b) l'indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami

Non è indicato

c) le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Presente: In caso di problemi nella evasione di un ordine, non esitate a contattarci. Inviare una e-mail con informazioni sul vostro ordine a it-support@pdassi.it.

d) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno

Non è indicato

e) l'indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;

Non è indicato

f) le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Non è indicato

g) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno

Non è indicato

2) Diritto di recesso

Verifica se il consumatore è informato dal venditore sui seguenti aspetti:

g) modalità esercizio del diritto di recesso o di esclusione dello stesso;

Non è indicato

h) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

Non è indicato

i) c)informazione sulle condizioni e le modalità di esercizio del diritto di recesso;

Non è indicato

j) indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;

Non è indicato

k) informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;

Presente

l) le condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno.

Non è indicato

3.2.3 D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali)

Gli obblighi del professionista è quello di rendere disponibile l'informativa sull'utilizzo dei dati del cliente(art. 13). Da quanto si evince dal

sito bancariaeditrice.it l'accesso all'informativa su l'utilizzo dei dati personali dal sito e dei diritti del consumatore è visionabile solo nel momento della registrazione, non essendoci un accesso successivo (es. attraverso un link ad una pagina). Verificato:

a) le finalità e le attività del trattamento cui sono destinati i dati;

Presente: pdassi non vende, noleggia o cede a terzi le tue informazioni personali. Queste vengono utilizzate esclusivamente per il trattamento degli ordini. NON riceverete nessuna pubblicità o messaggio di posta elettronica da pdassi dopo avere inserito le vostre informazioni personali.

b) la natura obbligatoria o facoltativa del conferimento dei dati;

Non è indicato

c) le conseguenze di un eventuale rifiuto di rispondere;

Non è indicato

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

Presente

e) diritto di accesso dell'interessato ai propri dati personali (art. 7);

Non è indicato

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le attività attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Non è indicato

3.2.4 Considerazioni.

Il sito pdassi.it appartiene ad una società tedesca (envi.con KG- Emser Platz 2, D-10719 Berlin Germania), quindi soggetta alla normativa italiana che è conforme a quella europea. Il sito non è a norma, necessita un urgente adeguamento.

CAPITOLO XI

LUCA ISMAELE LODRINI

LA TUTELA DEI NOMI A DOMINIO

SOMMARIO: 1. Considerazioni introduttive. – 2. Natura giuridica. – 3. Rapporti con il marchio. – 4. Tutela stragiudiziale. – 5. L'arbitrato irrituale. – 6. La procedura di riassegnazione. – 7. Tutela giudiziale.

1. Considerazioni introduttive.

Il nome a dominio consiste tecnicamente in una sequenza di numeri, atti ad identificare un determinato indirizzo IP, generalmente riconducibile ad un sito internet; detta sequenza di numeri è tradotta in una combinazione alfanumerica, cioè il nome a dominio così come comunemente inteso, il quale rappresenta anche, ma non solo, un indirizzo elettronico e, secondo alcuni²²⁸, un vero e proprio domicilio informatico; esso può anche essere definito come una “una serie di stringhe separate da punti” dove “la parte più importante è la prima partendo da destra”²²⁹, e cioè il c.d. top level domain (TLD); esso può essere tematico (ad es. .gov, .com) o geografico (.it, .uk, e così via); il TLD è seguito da un second level domain (SLD), che si identifica con la stringa alfanumerica liberamente (nel rispetto di alcuni criteri tecnici e normativi) determinata da colui che richiede la registrazione; è su tale parte del nome a dominio che comunemente si incentrano le controversie ed è su di essa che, di conseguenza, si concentra la tutela.

L'assegnazione del nome a dominio è, in via generale, governata dal principio “*first come first served*” e segue, quindi, l'ordine cronologico delle richieste; tuttavia l'assegnazione, nonchè il mantenimento della titolarità del nome a dominio, sono altresì subordinati al rispetto di una serie di ulteriori criteri, i quali trovano fondamento nella legge²³⁰, nonchè nelle c.d. “regole di naming”.

2. Natura giuridica

Il nome a dominio è attualmente considerato, a tutti gli effetti, un segno distintivo, per quanto atipico, al pari del marchio, ed un bene economico vero

²²⁸ Pieremilio Sammarco, “La tutela giudiziaria del nome a dominio in Italia” presso il sito internet <http://www.fog.it/convegni/programmi/03-05-30-rel-Sa.rtf>.

²²⁹ http://it.wikipedia.org/wiki/Domain_name_system#Nomi_DNS.

²³⁰ Ad es., il nome a dominio non deve contenere denominazioni riservate (es. Comune di Roma); non deve porsi in contrasto con quanto dettato dal D.Lgs. 10 febbraio 2005 n. 30, in tema di conflitti con gli altri segni distintivi; non deve contenere denominazioni generiche o descrittive, in quanto le stesse possono essere assunte ad indici di mala fede nella registrazione e, quindi, comprovare un intento speculativo.

e proprio, specialmente quando sia riconducibile ad una attività economica caratterizzata da un marchio di particolare valenza distintiva nonché di rinomanza e potere di attrattiva; caratteristiche che, appunto, analogamente a quanto avviene per il marchio, si estendono al nome a dominio.

Il recente D. Lgs. 10 febbraio 2005, n. 30, c.d. “Codice della proprietà industriale”, fa espresso riferimento al nome a dominio, nell'art. 12, ove si esclude che un segno distintivo possa definirsi “nuovo” quando sia identico o simile ad altri segni distintivi già noti, quali ad es. la ditta, l'insegna²³¹ e, fra gli altri, appunto, il nome a dominio; nell'art. 22, laddove si fa divieto di *“adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale un segno uguale o simile all'altrui marchio”*, qualora da ciò possa derivare confusione; infine nell'art. 118, ove si prevede che *“salvo l'applicazione di ogni altra tutela, la registrazione di nome a dominio aziendale concessa in violazione dell'articolo 22 o richiesta in mala fede, può essere, su domanda dell'avente diritto, revocata oppure a lui trasferita da parte dell'autorità di registrazione”*.

La competente Autorità di Registrazione, per i domini con ccTLD .it, è la Registration Authority (afferente al CNR di Pisa), la quale dal 1 febbraio 2004, e cioè dal momento in cui ha cessato di operare la Naming Authority, è anche l'autorità preposta alla formazione delle regole di naming (ora “Regolamento di Assegnazione”- RDA, versione 4.0 fino al mese di ottobre 2006; versione 5.0 dal mese di ottobre 2006²³²), oltre che alla loro applicazione. Detta autorità, in realtà, è tale solo nominalmente, avendo infatti natura giuridica di associazione non riconosciuta, pur assolvendo ad un interesse generale della collettività.

3. Rapporti con il marchio

Il principale segno distintivo con il quale il nome a dominio può entrare in conflitto, è indubbiamente il marchio. Il notevole interesse, manifestato dagli operatori commerciali, alla registrazione di un nome a dominio corrispondente alla propria denominazione, insegna o marchio, conferma l'importanza della valenza distintiva del nome a dominio; interesse, peraltro, senza dubbio meritevole di protezione da parte dell'ordinamento giuridico, sotto diversi profili tra cui, più evidenti, quello della tutela del consumatore contro la possibile confusione ingenerata dalla somiglianza di un nome a dominio con un corrispondente marchio rinomato, così come sotto il profilo della tutela dell'imprenditore da fattispecie di concorrenza sleale (art. 2598 c.c. e seguenti), e ciò sia nel caso in cui il nome a dominio sia inerente ad attività

²³¹ Così Trib. Reggio Emilia che, con ordinanza del 30 maggio 2000 considera il nome a dominio alla stregua di una insegna, o di uno spazio virtuale, e non di un mero indirizzo destinato esclusivamente ad identificare un singolo computer, come invece ritenuto dalla precedente giurisprudenza.

²³² Dal mese di ottobre 2006, infatti, entrerà in vigore in nuovo Regolamento di assegnazione, versione 5.0, ed il Regolamento per la risoluzione delle dispute nel ccTLD “it”, versione 1.0. Fonte: <http://www.nic.it/RA/novita/comunicazioni.html>

commerciali afferenti a settori di beni e/o servizi analoghi a quelli riferibili ad un marchio noto, sia nel diverso caso in cui, pur esercitando una attività commerciale in un settore non omogeneo, il titolare del nome a dominio analogo al marchio altrui, sfrutti la rinomanza di quest'ultimo per trarne un indebito vantaggio (ad es., anche attraverso pratiche quali il c.d. “typosquatting”²³³).

Il problema dei rapporti tra marchio e nome a dominio, in sintesi, si pone dunque sotto un duplice profilo: quello del rapporto fra il marchio ed un nome a dominio avente specifica funzione economica, e quello del rapporto con un nome a dominio che non abbia una funzione economica²³⁴. Se il primo caso, come già accennato, può essere risolto alla luce dei principi di correttezza e lealtà, che devono informare l'attività commerciale, e quindi la materia sarà disciplinata, come sopra indicato, dagli artt. 2598 c.c. e seguenti, dal R.D. 21 giugno 1942 e successive modifiche, nonché dal citato Codice della proprietà industriale, con generale prevalenza del marchio noto (preesistente) sul nome a dominio avente funzione economica, diversa soluzione occorre dare al caso in cui, non avendo il nome a dominio specifica funzione economica, ma afferendo ad es. al nome del registrante, che eserciti attraverso il relativo sito internet il proprio diritto, costituzionalmente garantito (art. 21), alla manifestazione del pensiero, o che lo utilizzi a fini di condivisione di opinioni od interessi; in questi casi, si deve propendere per la prevalenza dei diritti costituzionalmente garantiti della persona, nonché del diritto al nome, ed alla relativa tutela, di cui agli artt. 6 e 7 del codice civile, anche come espressione dell'identità individuale, su quelli di natura economica, di cui sopra.

La funzione assolta da uno specifico nome a dominio, economica o meno, vale altresì a qualificare il diritto, che su di esso insiste, come diritto di privativa, nel primo caso (soggetto alla tutela di cui all'art. 2598 c.c.), o di esclusiva, nel secondo; in tale ultima ipotesi, a seconda dei casi, potrà essere esperita l'azione di reclamo, o quella di usurpazione²³⁵. La risoluzione delle singole controversie, in caso di conflitto o interferenze del nome a dominio con il marchio e, più in generale, con gli altri segni distintivi, è tuttavia subordinata, nella pratica, all'esame specifico della fattispecie concreta.

4. Tutela stragiudiziale

²³³ *“L'attività definita "typosquatting" consiste nella pratica di chi effettua una registrazione di un nome a dominio molto simile ad altri domini noti e conosciuti, differenziandosi da questi ultimi per minime differenze letterali, riferibili a comuni errori di digitazione dell'utente di Internet. Tale pratica non può che costituire un'attività in mala fede”.* Fonte: <http://www.altalex.com/index.php?idnot=7114>.

²³⁴ Ad es. nel caso in cui il nome a dominio corrisponda al nome di un determinato soggetto, che ne faccia un uso non commerciale, ovverosia “personale” (sito internet che ospiti il resoconto delle proprie vacanze, oppure nel quale il registrante esteri le proprie opinioni, ecc.).

²³⁵ *“Mentre l'azione di reclamo di nome protegge l'uso del nome a favore della persona cui il nome spetta, l'azione di usurpazione di nome protegge l'esclusività dell'uso del nome a favore della stessa persona”.* Pieremilio Sammarco, op. cit., pag. 6, <http://www.fog.it/convegni/programmi/03-05-30-rel-Sa.rtf>.

La prima tutela che riceve il nome a dominio, ha natura “preventiva”; la registrazione del nome (con TLD .it) presso la RA italiana, infatti, come già sopra accennato, è subordinata al rispetto di una serie di criteri, o regole²³⁶, elencati nel sito della medesima RA; tralasciando le regole puramente tecniche, i principali criteri sono:

1) il carattere esclusivo e riservato di alcune categorie di denominazioni, e principalmente: a) nomi riservati geografici; b) nomi riservati di utilizzo generale; c) nomi riservati di pubblica amministrazione; nonché altri nomi riservati contenuti in una elencazione più dettagliata²³⁷, sempre afferenti alla P.A.;

2) nel rispetto delle regole indicate, l'ordine cronologico delle richieste.

La RA, quindi, non può dar seguito alle richieste di registrazione di nomi a dominio, afferenti alle categorie sopra elencate, che provengano da soggetti non legittimati²³⁸. In ogni altro caso, anche al fine di prevenire casi di c.d. “cybersquatting”²³⁹, l'espletamento della procedura di registrazione è subordinata alla sottoscrizione di una lettera di assunzione di responsabilità, dal parte del richiedente, con la quale egli dichiara di “*avere titolo all'uso e/o disponibilità giuridica del nome a dominio richiesto e di non ledere, con tale richiesta di registrazione, diritti dei terzi*”.

La tutela “successiva”, approntata dalla RA a garanzia delle legittimità della registrazione e del mantenimento del nome a dominio, trova anch'essa fondamento nella lettera di assunzione di responsabilità²⁴⁰, con la

²³⁶ <http://www.nic.it/RA/domini/regole.html>

²³⁷ <http://www.nic.it/NA/nomi-riservati-curr.html>

²³⁸ In realtà le Autorità di registrazione, compresa quella italiana, non compiono autonomamente, di regola, controlli sulla legittimità del richiedente all'uso del nome a dominio, salvo il caso di nomi non assegnabili, come quelli riservati alla P.A.; per gli altri casi, le Autorità sopperiscono con le c.d. “LAR”, cioè lettere di assunzione di responsabilità.

²³⁹ “L'espressione anglosassone **cybersquatting** o anche **domain grabbing** (da *to grab* = *ghermire*) indica il fenomeno di accaparramento di nomi di dominio corrispondenti a marchi altrui o a nomi di personaggi famosi al fine di realizzare un lucro sul trasferimento del dominio a chi ne abbia interesse”. Fonte: <http://it.wikipedia.org/wiki/Cybersquatting>.

²⁴⁰ All'indirizzo http://www.nic.it/RA/domini/lettere_ar.html sono presenti due modelli, a seconda che il richiedente sia persona fisica oppure soggetto diverso da persona fisica; in entrambi i casi è richiesta la doppia sottoscrizione ex artt. 1341 – 1342 c.c., con espresso riferimento all'accettazione dell'art. 14 del Regolamento di Assegnazione, relativo alla Risoluzione delle dispute, nonché alla rinuncia al risarcimento dei danni nei confronti della R.A. per l'eventuale revoca del nome a dominio; è appena il caso di accennare che, tuttavia, l'espressa approvazione delle clausole vessatorie, benchè valida ed efficace nei confronti di soggetto che non rivesta la qualità di consumatore, alla luce dell'art. 1469 bis c.c. nonché del recente “Codice del Consumo” (D. Lgs. n. 206/2005), presenta in realtà notevoli margini di incertezza, la fattispecie potendo in effetti rientrare nell'ambito di applicazione delle c.d. “nullità di protezione”, introdotte dal citato D. Lgs. n. 206/2005 (art. 36), che, peraltro, prevede come assolutamente inderogabile il foro del consumatore nelle contrattazioni a distanza (e, in effetti, la richiesta di registrazione del nome a dominio avviene a distanza), nonché come parzialmente inderogabile il medesimo foro, in casi diversi dalla contrattazione a distanza, laddove una deroga la suddetto principio sarebbe in via teorica possibile solo a seguito di espressa trattativa individuale fra le parti, con onere della prova incombente sul professionista (RA) - (la sussistenza di tale trattativa, è in via di principio da escludersi quando la deroga sia contenuta in moduli o formulari unilateralmente predisposti dal professionista, quale è appunto la lettera di assunzione di responsabilità). Non pare possa fondatamente dubitarsi, peraltro,

sottoscrizione della quale il richiedente si assoggetta al Regolamento di Assegnazione, “*ivi esplicitamente inclusa la parte relativa alla Risoluzione delle dispute*”; l'accettazione espressa, ex artt. 1341 – 1342 c.c., delle condizioni di risoluzione delle dispute (art. 14 RDA), quantomeno da parte di soggetti diversi da persone fisiche qualificabili come consumatori, cioè da operatori professionali, segna i successivi passi nella tutela stragiudiziale del nome a dominio, che può seguire la duplice via dell'arbitrato irrituale, di cui all'art. 15 RDA, oppure della procedura di riassegnazione, di cui all'art. 16 del medesimo Regolamento.

Entrambi questi rimedi presuppongono l'introduzione, presso la RA, della procedura di contestazione (art. 14 RDA), ed ovviamente che questa non si risolva amichevolmente; in caso di bonaria risoluzione, in questa fase della procedura, la RA, a seconda dei casi, procederà alla cancellazione della notazione “valore contestato”, apposta nel Registro accanto al nome a dominio oggetto di controversia, al momento della ricezione della contestazione; oppure procederà alla rimozione della assegnazione del nome a dominio contestato, dopo averlo reso indisponibile alla registrazione per trenta giorni, in attesa della richiesta della parte a cui favore si sia risolta la procedura di contestazione. Nel caso tale procedura non si concluda con un accordo amichevole, entro dieci giorni lavorativi dalla ricezione della contestazione, che deve contenere gli elementi di cui all'art. 14.1²⁴¹ RDA, la RA invita le parti a dare inizio alla procedura arbitrale o a quella di riassegnazione di cui all'art. 16.

4.1 L'arbitrato irrituale

L'art. 15.1 del RDA prevede la possibilità, per il richiedente, di impegnarsi fin dalla sottoscrizione della lettera di assunzione di responsabilità, od anche successivamente, a devolvere ad arbitrato irrituale le eventuali controversie connesse alla assegnazione del nome a dominio richiesto, “*riconoscendo come valide e vincolanti le decisioni prese dal collegio arbitrale*”.

La scelta di questa via alternativa di risoluzione delle dispute, è quindi lasciata alla libera volontà delle parti; il registrante, infatti, “*può*” impegnarsi a devolvere ad un arbitrato irrituale la risoluzione della controversia; potrebbe, d'altra parte, scegliere invece la via della tutela giudiziaria ordinaria; a sua volta, il soggetto che dovesse ritenersi leso dalla assegnazione ad altri di un determinato nome a dominio, nel caso in cui optasse a sua volta per l'arbitrato irrituale, dovrebbe verificare se, nel database della NA, accanto al nome a dominio assegnato, vi sia menzione circa la preferenza espressa dal registrante in ordine alla devoluzione delle controversie, appunto, all'arbitrato irrituale.

della natura professionale della attività della RA e della qualifica, da questa rivestita, di “professionista”, in accordo con la definizione contenuta nell'art. 3 lettera c) del Codice del Consumo.

²⁴¹ “*La lettera di contestazione deve contenere le generalità del mittente, il nome a dominio contestato, i motivi della contestazione, il pregiudizio subito dal mittente o il proprio diritto che questi assume leso*”.

Occorre evidenziare, in ogni caso, che il soggetto contestante è terzo rispetto al rapporto contrattuale intercorrente fra la RA ed il richiedente e che pertanto non sarebbe tenuto ad aderire alla preferenza espressa dal richiedente per l'arbitrato o eventualmente per la procedura di riassegnazione, potendo invece liberamente adire l'autorità giudiziaria.

Presso la RA è costituito un elenco di arbitri, tra i quali le parti devono scegliere il proprio (art. 15.3 RDA²⁴²); i due arbitri di parte scelgono poi di comune accordo il terzo arbitro, che rivestirà la funzione di presidente del collegio arbitrale. La decisione deve intervenire entro novanta giorni dalla costituzione del collegio arbitrale. Lo scambio di memorie e di repliche fra le parti, può poi avvenire per posta elettronica, salvo espressa richiesta della forma cartacea o, eventualmente, per quella documentazione non trasmissibile, per sua natura, via e-mail.

L'art. 15.5 stabilisce poi i poteri degli arbitri, i quali, ricorrendone le condizioni e ad istanza di parte, possono assumere provvedimenti cautelari, in relazione al nome a dominio contestato, e la RA è tenuta a dare immediata esecuzione a tali provvedimenti. La decisione del collegio arbitrale, adottata sulla base del RDA e dell'Ordinamento Italiano, è inappellabile nel merito (art. 15.6 RDA); con la decisione, gli arbitri liquidano anche il loro compenso e le spese, che pongono in tutto o in parte a carico del soccombente (art. 15.7).

4.2 La procedura di riassegnazione

In alternativa alla procedura arbitrale, in presenza di contestazione del nome a dominio, chi contesta può optare per la procedura di riassegnazione (art. 16 RDA); tale procedura, che non ha natura giurisdizionale, non pregiudica l'eventuale ricorso delle parti all'Autorità giudiziaria ordinaria o al Collegio arbitrale e può essere attivata dal ricorrente a prescindere dalla procedura di risoluzione delle controversie eventualmente indicata dalla controparte assegnataria, nella lettera di assunzione di responsabilità o successivamente; non può essere attivata, invece, se sia già pendente, in relazione al nome a dominio contestato, altra procedura di fronte alle predette autorità. In ogni caso il resistente conserva comunque la possibilità di rivolgersi, come detto, all'Autorità giudiziaria o al Collegio arbitrale.

Nell'ambito della procedura di riassegnazione, il cui scopo è la verifica della legittimazione in ordine alla disponibilità giuridica del nome a dominio da parte dell'assegnatario²⁴³, le contestazioni vengono devolute ai c.d. "Enti

²⁴² La nomina dell'arbitro di parte deve avvenire a mezzo lettera raccomandata A/R, indirizzata all'arbitro prescelto, alla controparte ed alla RA; la lettera deve altresì contenere l'oggetto della domanda, le ragioni di fatto e di diritto su cui si fonda, le conclusioni, il proprio domicilio e l'indirizzo di posta elettronica, nonché l'invito alla controparte a nominare il proprio arbitro. La controparte, a sua volta, entro dieci giorni lavorativi dalla ricezione della raccomandata dovrà nominare, con le stesse modalità, il proprio arbitro; i due arbitri, così indicati, dovranno poi entro cinque giorni lavorativi nominare il presidente.

²⁴³ Art. 11.6 RDA: "La Procedura ha come scopo la verifica del titolo all'uso o alla disponibilità giuridica del nome a dominio, e che il dominio non sia stato registrato e mantenuto in mala fede. L'esito della procedura può essere solo la riassegnazione di un nome a dominio. La procedura non ha

conduttori”²⁴⁴, composti da almeno quindici esperti in materia, c.d. “saggi”. La procedura avanti gli Enti conduttori, prevede che la controversia sia devoluta, a scelta del ricorrente, ad un collegio di tre saggi, oppure ad un unico saggio; le relative spese sono interamente a carico del ricorrente, diversamente da quanto accade in ambito arbitrale (ove seguono, in tutto o in parte, la soccombenza).

L'art. 16.6 del RDA individua le condizioni in base alle quali è possibile sottoporre a procedura un determinato nome a dominio; ciò avviene quando il dominio sia “*identico o tale da indurre confusione rispetto ad un marchio su cui egli vanta diritti, o al proprio nome e cognome*”; che “*l'attuale assegnatario non abbia alcun diritto o titolo in relazione al nome a dominio contestato*”; che “*il nome a dominio sia stato registrato e venga usato in mala fede*”.

L'eventuale titolo di legittimazione alla registrazione (lettera b), da parte dell'assegnatario, è verificabile attraverso l'utilizzo dei parametri di cui alla seconda parte dell'art. 16.6²⁴⁵. La sussistenza di una serie di circostanze, meramente esemplificative, previste dall'art. 16.7²⁴⁶, costituisce prova di mala fede nella registrazione e nell'uso del nome a dominio; principalmente, esse si

natura giurisdizionale, e come tale non preclude alle parti il ricorso, anche successivo, alla magistratura o all'arbitrato previsto dall'articolo 15 del presente Regolamento”.

²⁴⁴ “*La procedura è condotta da apposite organizzazioni, persone giuridiche pubbliche o private o studi professionali costituite nell'Unione Europea, chiamate enti conduttori e rispondenti ai requisiti predisposti dal Registro previo parere della Commissione Regole*” <http://www.nic.it/RA/domini/contestazione.html>; l'elenco degli attuali Enti conduttori, o PSRD (Prestatori del Servizio di Risoluzione delle Dispute, così come definiti nella nuova versione 5.0 del RDA) è consultabile all'indirizzo: <http://www.nic.it/RA/domini/contestazioni/entiConduttori.html>

²⁴⁵ “*In relazione al precedente punto “b)” del presente articolo, il resistente sarà ritenuto avere diritto o titolo al nome a dominio contestato qualora provi che:*

a) prima di avere avuto notizia della contestazione in buona fede ha usato o si è preparato oggettivamente ad usare il nome a dominio od un nome ad esso corrispondente per offerta al pubblico di beni e servizi; oppure

b) che è conosciuto, personalmente, come associazione o ente commerciale con il nome corrispondente al nome a dominio registrato, anche se non ha registrato il relativo marchio; oppure

c) che del nome a dominio sta facendo un legittimo uso non commerciale, oppure commerciale senza l'intento di sviare la clientela del ricorrente o di violarne il marchio registrato”.

²⁴⁶ “*Le seguenti circostanze, se dimostrate, saranno ritenute prova della registrazione e dell'uso del dominio in mala fede:*

a) circostanze che inducano a ritenere che il nome a dominio è stato registrato con lo scopo primario di vendere, cedere in uso o in altro modo trasferire il nome a dominio al ricorrente (che sia titolare dei diritti sul marchio o sul nome) o ad un suo concorrente, per un corrispettivo, monetario o meno, che sia superiore ai costi ragionevolmente sostenuti dal resistente per la registrazione ed il mantenimento del nome a dominio;

b) la circostanza che il dominio sia stato registrato dal resistente per impedire al titolare di identico marchio di registrare in proprio tale nome a dominio, ed esso sia utilizzato per attività in concorrenza con quella del ricorrente;

c) la circostanza che il nome a dominio sia stato registrato dal resistente con lo scopo primario di danneggiare gli affari di un concorrente o di usurpare nome e cognome del ricorrente;

d) la circostanza che, nell'uso del nome a dominio, esso sia stato intenzionalmente utilizzato per attrarre, a scopo di trarne profitto, utenti di Internet creando motivi di confusione con il marchio del ricorrente”.

identificano con la volontà di registrare il dominio non ai fini di un diretto utilizzo, ma al solo scopo di rivenderlo o trasferirlo al soggetto che sarebbe invece legittimato a detenerlo, o ad un suo concorrente, al fine di danneggiare l'altrui iniziativa economica, o di trarre ingiusto profitto dalla rinomanza del nome altrui. La decisione dei saggi sarà eseguita dalla RA qualora, entro quindici giorni dalla data di ricezione della decisione stessa, non abbia ricevuto comunicazione di ricorso alla Autorità giudiziaria ordinaria da parte del resistente.

5. La tutela giudiziale

Il ricorso all'autorità giudiziaria, in alternativa alla procedura arbitrale o di riassegnazione, è sempre possibile per il reclamante; da un punto di vista pratico la via giudiziaria si presenta più lunga e più costosa, certamente meno idonea a soddisfare le necessità di celerità e speditezza proprie di una azienda, soprattutto di una azienda attiva nel campo dell'e-commerce. Ciò nonostante, il ricorso all'autorità giudiziaria presenta anche dei vantaggi; il vincitore, oltre ad ottenere la riassegnazione del nome a dominio, può, nella medesima sede (di merito), chiedere che gli vengano liquidati i danni, senza dover intraprendere un nuovo giudizio.

Ricorrendone i presupposti (*“pregiudizio imminente e irreparabile”*), colui che richiede la riassegnazione del nome a dominio, può agire in via d'urgenza ex art. 700 c.p.c., chiedendo al Giudice i *“provvedimenti d'urgenza, che appaiono, secondo le circostanze, più idonei ad assicurare provvisoriamente gli effetti della decisione sul merito”*; sicchè, in via d'urgenza, il ricorrente potrà richiedere l'inibitoria all'uso del nome a dominio da parte dell'assegnatario, per poi chiedere, nel successivo giudizio di merito, la riassegnazione dello stesso, anche sulla scorta dell'art. 133 D.Lgs. n. 30/2005²⁴⁷ (*“Codice della proprietà industriale”*, *“Tutela cautelare dei nomi a dominio”*) ed il risarcimento del danno.

La tutela giudiziaria può essere ottenuta anche sotto il profilo della repressione degli atti di concorrenza sleale, sotto quello della violazione del principio di correttezza nell'esercizio dell'attività professionale, sia sotto quello dell'utilizzo di segni distintivi idonei a produrre confusione con segni distintivi altrui²⁴⁸; detta tutela può avvenire innanzi le Sezioni specializzate in materia di proprietà industriale ed intellettuale presso Tribunali e Corti d'Appello, istituite dal Decreto Legislativo 27 giugno 2003, n. 168. E' infine solo il caso

²⁴⁷ *“L'Autorità giudiziaria può disporre, in via cautelare, oltre all'inibitoria dell'uso del nome a dominio aziendale illegittimamente registrato, anche il suo trasferimento provvisorio, subordinandolo, se ritenuto opportuno, alla prestazione di idonea cauzione da parte del beneficiario del provvedimento”*.

²⁴⁸ Art. 2598 c.c.: *“Ferme le disposizioni che concernono la tutela dei segni distintivi (2563 ss., 2568, 2569 ss.) e dei diritti di brevetto (2584 ss., 2592, 2593), compie atti di concorrenza sleale chiunque: 1) usa nomi o segni distintivi idonei a produrre confusione (2564) con i nomi o con i segni distintivi legittimamente usati da altri, o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti e con l'attività di un concorrente...”*.

di accennare che condotte integranti fattispecie di concorrenza sleale, relative al nome a dominio come segno distintivo, potrebbero configurare una responsabilità penale ex art. 517 c.p.²⁴⁹; l'utilizzo del nome altrui (persona fisica o giuridica), potrebbe d'altra parte altresì configurare un'ipotesi di trattamento illecito di dati personali e la relativa tutela sarebbe azionabile, alternativamente, avanti l'Autorità giudiziaria ordinaria, oppure avanti l'Autorità Garante per il trattamento dei dati personali.

²⁴⁹ “Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno (2575-2594) o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri (2563-2574), atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa fino a € 1.032”.

CAPITOLO XII

MARIA MANICCIA

LA CONSERVAZIONE DELLE SCRITTURE CONTABILI IN
FORMATO DIGITALE

SOMMARIO: 1. Considerazioni introduttive. - 2. Archiviazione e conservazione in ambiente digitale. - 3. Il processo di conservazione sostitutiva: oggetto e finalità. - 4. Documenti informatici, documenti analogici unici e non unici. - 5. La conservazione sostitutiva dei documenti informatici rilevanti ai fini tributari. - 6. I documenti informatici rilevanti ai fini tributari - ambito di applicazione del Decreto ministeriale 23 gennaio 2004. - 7. Le caratteristiche dei documenti informatici rilevanti ai fini tributari: formazione emissione, esibizione e memorizzazione. - 8. Il processo di conservazione dei documenti informatici rilevanti ai fini tributari. - 9. Il riversamento e l'esibizione dei documenti informatici rilevanti ai fini tributari. - 10. La tenuta e la conservazione sostitutiva delle scritture contabili. - 11. Tenuta delle scritture contabili con modalità informatiche. 12. conservazione delle scritture contabili con modalità informatiche. - 13. Conservazione sostitutiva di scritture contabili stampate su supporto cartaceo. - 14. Invio dell'impronta all'Amministrazione finanziaria. - 15. Esempi di procedimenti di conservazione di scritture contabili. - 16. Il responsabile della conservazione. - 17. L'intervento del pubblico ufficiale. - 18. Il manuale della conservazione. - 19. I supporti per la conservazione sostitutiva in formato digitale. - 20. Conclusioni.

1 Considerazioni introduttive.

Il rinnovamento dell'impianto amministrativo tributario finalizzato ad una progressiva agevolazione delle modalità di adempimento degli obblighi prescritti dalla normativa fiscale, tale da consentire l'archiviazione e conservazione informatizzata dei documenti nonché l'emissione di veri e propri documenti informatici, si inquadra nel più ampio e generalizzato movimento di semplificazione amministrativa risalente ai primi anni '90.

Era infatti il 1994 quando, con il terzo comma dell'articolo 2220²⁵⁰ del codice civile, così come novellato dall'art. 7 bis del decreto legge 10 giugno 1994 n. 357 convertito dalla legge 8 agosto 1994, n. 489, il legislatore introduceva nel nostro ordinamento la possibilità di conservare *scritture e documenti contabili* sotto forma di registrazioni su supporti di immagine, pur

²⁵⁰ Art. 2220 c.c. - c.1 - Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione.

c. 2 - Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.

c. 3 - Le scritture e i documenti dei cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti.

con il vincolo che le registrazioni corrispondessero ai documenti e potessero essere trasformate in qualsiasi momento in un esemplare leggibile del documento di origine.

L'ultimo comma del citato art. 7 bis estendeva inoltre l'applicazione della nuova normativa a tutte le scritture e i documenti rilevanti ai fini tributari rinviando ulteriori disposizioni per la conservazione su supporti di immagine ad un apposito Decreto da emanarsi a cura del Ministero delle Finanze.

La disciplina che ha reso operativa l'introdotta novità è stata emanata dal Ministero dell'Economia e delle Finanze soltanto dieci anni dopo con il D.M. 23 gennaio 2004.

Il citato decreto regola le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto, occupandosi di disciplinarne l'emissione, la conservazione e l'esibizione siano essi *ab origine* documenti informatici o analogici. Nel decreto sono contenute disposizioni che implementano, secondo le esigenze più rigorose imposte dalla materia fiscale, quelle previste dalla deliberazione CNIPA n. 11/2204 del 19 febbraio 2004²⁵¹ recante, a sua volta, le "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali".

Un ulteriore e definitivo impulso nei confronti di una progressiva e generalizzata adesione a nuove modalità tecnico-informatiche in materia di formazione, trasmissione, archiviazione, conservazione dei documenti e non solo, è rappresentato dal *Codice dell'amministrazione digitale*²⁵² che ha sensibilmente contribuito a consolidare quei principi attinenti la dematerializzazione dei documenti che erano già stati sanciti dal Testo Unico sulla documentazione amministrativa emanato con il DPR 28/12/2000 n. 445 ed in gran parte aggiornato proprio dal dlgs 7/3/2005, n. 82.

Il Codice dell'Amministrazione digitale prevede, tra l'altro, che le pubbliche amministrazioni ed i privati possano *formare* e *conservare* su supporti informatici libri, repertori e scritture di cui sia obbligatoria la tenuta (art. 39, c. 1) ovvero *sostituire* i documenti degli archivi, le scritture contabili, la corrispondenza e ogni atto o documento di cui è prescritta la conservazione per legge o regolamento nel caso essi vengano riprodotti su supporti informatici attraverso modalità tali da garantirne la conformità agli originali e la conservazione nel tempo (art. 41, c. 1); il Cad inoltre riconosce efficacia probatoria e pieno valore legale (ai sensi dell'art. 2702 c.c.) al documento informatico sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata (art. 21, c. 2²⁵³).

²⁵¹ La deliberazione CNIPA n. 11/2004 ha integralmente sostituito la deliberazione AIPA 13 dicembre 2001, n. 42.

²⁵² Emanato con decreto legislativo 7 marzo 2005, n. 82 e aggiornato con disposizioni integrative e correttive dal D.lgs n. 159 del 4 aprile 2006.

²⁵³ Art. 21, c. 2 del d.lgs 82/2005: Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'art. 2702 del codice civile.

Per restringere l'argomento al più circoscritto ambito fiscale, l'art. 21 comma 5²⁵⁴ del codice dell'amministrazione digitale infine prevede che gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto vengano assolti secondo le modalità definite con uno o più decreti del ministro dell'Economia e delle Finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

A concludere l'iter fiscale di questa nuova disciplina, inaugurata dai principi sanciti dall'art. 7 bis del decreto legge 10 giugno 1994 n. 357 e transitata per il Decreto ministeriale 23 gennaio 2004, è stata la Circolare interpretativa dell'Agenzia delle Entrate n. 36 del 6 dicembre 2006 che illustra le principali novità introdotte dal DMEF del 23 gennaio 2004 in tema di adempimenti fiscali relativi ai documenti informatici.

2 Archiviazione e conservazione in ambiente digitale

L'archiviazione elettronica e la conservazione digitale sono due distinti processi caratterizzati da una diversa natura e distinte modalità attuative.

In particolare per *archiviazione* elettronica si intende il processo di memorizzazione, su qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento (delibera Cnipa 11/2004 art. 1, c. 1 lett. g²⁵⁵).

L'*archiviazione* è inoltre un processo facoltativo, propedeutico a quello di conservazione e non vincolato all'osservanza di particolari obblighi imposti dalla normativa.

Il processo di *conservazione sostitutiva*, generalmente successivo all'eventuale archiviazione elettronica, permette di sostituire a tutti gli effetti di legge i documenti informatici e/o analogici oggetto del processo medesimo. Diversamente da quanto avviene per l'archiviazione, nella realizzazione della conservazione sostitutiva occorre attenersi ai rigidi dettami previsti dalla apposita disciplina ed in particolare, per quanto riguarda le scritture contabili ed i documenti informatici o analogici rilevanti ai fini tributari, alle disposizioni tecniche stabilite agli articoli 3 e 4 del DMEF più volte citato.

E' comunque consentito ai soggetti che ricorrono a tale modalità di conservazione dei documenti adottare accorgimenti e procedure integrative nonché scegliere i tipi di supporto purché nel rispetto delle norme di riferimento.

Può quindi affermarsi che il fine dell'archiviazione elettronica è quello

L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

²⁵⁴ Art. 21, c. 5 del d.lgs 82/2005: Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

²⁵⁵ Deliberazione Cnipa 11/2004 art. 1, c. 1 lett.) g *archiviazione elettronica*: processo di memorizzazione, su qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, così come individuati nella precedente lettera f), univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.

di permettere un facile, rapido e logico accesso a documenti archiviati e sottratti a voluminosi supporti cartacei, scopo della conservazione sostitutiva è quello ulteriore di rendere i documenti *non deteriorabili, disponibili nel tempo ed in formato integro ed autentico*.

3. Il processo di conservazione sostitutiva: oggetto e finalità

Oggetto di conservazione sostitutiva possono essere tanto i documenti informatici quanto quelli analogici anche se si deve anticipare che i procedimenti di conservazione previsti dalla normativa per queste due diverse categorie non sono perfettamente coincidenti differendo per talune modalità, adempimenti e tempistiche più avanti specificate.

Come già detto la finalità che caratterizza principalmente il processo di conservazione sostitutiva è rendere un documento non deteriorabile e quindi disponibile nel tempo in formato autentico ed integro.

Nondimeno, diversi sono i motivi e molteplici le finalità che possono indurre una impresa, una azienda ecc. a preferire la soluzione della conservazione in formato digitale delle scritture contabili e dei documenti rilevanti ai fini fiscali, tra i quali:

- una riduzione massiccia della giacenza cartacea ed una conseguente pressoché completa riduzione degli spazi occupati dagli atti cartacei;
- una modalità di individuazione e recupero della documentazione rapida e veloce che si traduce in una drastica riduzione dei tempi solitamente necessari con conseguente liberazione di risorse umane per attività di genere diverso;
- la possibilità per l'utente di disporre immediatamente delle informazioni contenute nei documenti;
- una consistente riduzione per l'impresa della spesa per la produzione di documenti cartacei soprattutto nel caso in cui alla conservazione sostitutiva si affianchi la contestuale organizzazione di un complessivo sistema di gestione documentale informatizzato;
- una notevole contrazione dell'out-put dell'azienda che può contribuire a calmierare i costi di gestione;
- l'opportunità di organizzare ed installare archivi capaci di garantire un elevato livello di sicurezza e riservatezza delle informazioni in essi contenute (cifratura degli archivi);
- l'opportunità di realizzare archivi sicuri costruiti su supporti autoconsistenti²⁵⁶.

Appare quindi chiaro come la possibilità di disporre di un sistema informativo in grado di gestire e conservare secondo le norme i documenti in forma digitale rappresenti sia per le Aziende Private sia per la Pubblica Amministrazione uno innovativo strumento di economia e di sviluppo.

²⁵⁶ Per *autoconsistenti* si intendono quei supporti dotati dal software necessario per le operazioni di ricerca e visualizzazione e quindi direttamente utilizzabili tramite PC.

4. Documenti informatici, documenti analogici unici e non unici

Prima di procedere all'esposizione del processo di conservazione sostitutiva è necessario trattare brevemente dei documenti informatici e dei documenti analogici le cui diverse caratteristiche incidono sulle modalità stesse del procedimento di conservazione previste dalla normativa.

Dal punto di vista giuridico il *documento informatico* è definito²⁵⁷ come “*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*”, mentre dal punto di vista *strutturale* esso è espressione di una sequenza di “*bit*” e, posto che una successione di “*bit*” si riproduce sempre uguale a se stessa, la natura medesima del documento informatico non permette di distinguerne l'originale dalla copia.

Diversamente per il documento analogico è di uso comune distinguere tra “documento originale” e “copia del documento originale”, così come fanno, peraltro anche la Delibera Cnipa 11/2004 e il Decreto Ministeriale 23/1/2004 sennonché, i citati testi normativi distinguono ulteriormente il *documento analogico originale* in “*unico*” e “*non unico*” a seconda sia possibile o meno risalire al suo contenuto attraverso altre scritture o documenti, anche in possesso di terzi, di cui sia obbligatoria la tenuta.

Per rimanere nell'ambito della tematica interessante la presente relazione, si possono indicare come esempi di documenti *analogici non unici*, fra le scritture tenute sia ai fini civilistici sia ai fini fiscali, i libri previsti dall'articolo 2214 c. 1 c.c.²⁵⁸ tra i quali ad esempio il *libro giornale* il cui contenuto può essere interamente ripristinato attraverso le schede di mastro la cui tenuta è appunto obbligatoria.

Altri esempi possono rinvenirsi in documenti contabili quali *fatture, ricevute fiscali, documenti di trasporto*, tutti da emettersi obbligatoriamente in duplice copia.

Documenti *analogici unici* possono invece considerarsi i *libri sociali* previsti dall'articolo 2421 c.c.²⁵⁹, infatti per conoscere il loro contenuto non può farsi riferimento ad altre scritture o documenti la cui conservazione sia obbligatoria, eccezion fatta per il caso in cui detti libri siano depositati presso gli archivi notarili, condizione questa che ne farebbe venire meno l'unicità.

Come già accennato le due differenti tipologie di documenti analogici assumono particolare rilievo in riferimento alle diverse modalità previste dalla normativa per il processo di conservazione.

In particolare, i documenti analogici originali non unici vengono trattati alla stregua delle copie e come questi affrancati dalle modalità prescritte per i documenti analogici originali unici ed in particolare dal processo di

²⁵⁷ Art. 1, c. 1 lett. d) deliberazione Cnipa 19 febbraio 2004; art. 1, c. lett. e del D.M. del Ministero dell'Economia e delle Finanze; art., 1 c. 1 lett. p) del d.lgs 82 del 7 marzo 2005.

²⁵⁸ Art. 2214 c.c. – c. 1 L'imprenditore che esercita un'attività commerciale deve tenere il libro giornale e il libro degli inventari

²⁵⁹ Libro dei soci, libro delle obbligazioni, libro delle adunanze e delle deliberazioni delle assemblee, libro delle adunanze e delle deliberazioni del consiglio di amministrazione, libro delle adunanze e delle assemblee degli obbligazionisti ecc.

conformità eseguito da un pubblico ufficiale che, per il settore privato, è da identificarsi quasi sempre con il notaio.

5. I documenti informatici rilevanti ai fini tributari – ambito di applicazione del D.M. 23/1/2004.

La disciplina introdotta dal già citato D.M. 23 gennaio 2004 si applica ai documenti rilevanti ai fini tributari ed in particolare alle scritture contabili, ai libri, ed ai registri previsti dalla normativa fiscale fra i quali si possono citare a titolo esemplificativo alcuni fra quelli previsti dal DPR 600/1973 e dal DPR 633/1972 quali:

- il libro giornale;
- il libro degli inventari;
- i libri previsti ai fini dell'imposta sul valore aggiunto (degli acquisti, dei corrispettivi e delle fatture emesse);
- i registri dei beni ammortizzabili ecc.

L'applicazione del DMEF si estende inoltre a tutte le dichiarazioni fiscali ed ai diversi modelli di pagamento (F24, F23 ecc.) predisposti dall'Amministrazione finanziaria.

Il decreto del Ministero dell'Economia e delle Finanze esclude dal proprio ambito di applicazione, per esplicita previsione dell' art. 2 comma 2²⁶⁰, le scritture contabili ed i documenti relativi al settore doganale, delle accise e delle imposte di consumo di competenza dell'Agenzia delle Dogane.

6. Le caratteristiche dei documenti informatici rilevanti ai fini tributari: formazione, emissione, esibizione e memorizzazione

Il D.M. 23 gennaio 2004 all'art. 3²⁶¹ fissa le caratteristiche dei documenti informatici rilevanti ai fini tributari ed indica gli obblighi da osservare riguardo la loro *formazione, emissione, memorizzazione, esibizione e conservazione*:

Formazione: *il documento statico non modificabile art.3 c. 1 lett. a)*

I documenti informatici rilevanti ai fini tributari hanno la *forma* di documenti statici non modificabili: la norma in pratica richiede che i documenti non risultino alterabili durante le fasi di accesso e di conservazione.

Per realizzare tale immutabilità è necessario che i documenti non contengano *macroistruzioni* e/o *codici eseguibili* (es. .doc, .xls, .ppt) .

Per *macroistruzioni* si intendono comandi interni al documento che al verificarsi di determinate condizioni generano automaticamente modificazioni dei dati contenuti. Un esempio è quello che può trarsi dal campo "*data*" che, nel momento in cui il documento viene aperto, salvato ecc., aggiorna

²⁶⁰ D.M. 23/1/2004 art. 2 c. 2: Il presente decreto non si applica alle scritture e ai documenti rilevanti ai fini delle disposizioni tributarie nel settore doganale, delle accise e delle imposte di consumo di competenza dell'Agenzia delle dogane.

²⁶¹ D.M. 23/1/2004 art. 3 comma 1 lett. a): I documenti rilevanti ai fini tributari:
a) hanno la forma di documenti statici non modificabili

automaticamente la data.

I *codici eseguibili* sono invece istruzioni, non sempre palesi all'utente, che permettono all'elaboratore di apportare modifiche al contenuto del documento informatico.

La normativa, conscia delle rapide evoluzioni che si susseguono in ambito tecnologico, non ha stabilito tassativamente quali siano i formati che garantiscono l'adempimento delle caratteristiche richieste e siano conseguentemente da adottare.

Gli utenti possono quindi rivolgersi a diversi formati tipici dei documenti digitali quali ad esempio l'Xml, il Txt o il Pdf/A²⁶² che attualmente sembra da ritenersi preferibile in quanto già ampiamente impiegato per l'invio di atti ufficiali da parte di intermediari ed imprese.

La scelta del formato da adottare per i documenti informatici rientra tra gli incarichi del *responsabile della conservazione*, una nuova figura di cui si dirà più avanti, che è tenuto a garantire l'integrità e l'effettiva leggibilità dei documenti per tutto il tempo in cui questi devono essere conservati.

Anche le scritture contabili possono essere "formate" come documenti statici non modificabili.

Emissione art. 3 comma 1 lett. b)

La seconda caratteristica dei documenti informatici rilevanti ai fini tributari stabilita dall'art.3 c. 1 lett. b)²⁶³ del D.M. 23 gennaio 2004 riguarda la loro emissione che, al fine di assicurare la *data*, l'*integrità* ed *autenticità* dei documenti medesimi, deve essere eseguita attraverso l'apposizione del *referimento temporale*²⁶⁴ e della *sottoscrizione elettronica* definiti rispettivamente: il primo come ***l'informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici*** (art. 1 c. 1 lett. p del decreto 23 gennaio 2004, art. 1 c. 1 lett. p della delibera Cnipa 11/2004 e art. 1 del DPCM 13 gennaio 2004 art. 1 lett. g); la seconda come ***l'apposizione della firma elettronica qualificata*** ovvero la ***firma digitale***²⁶⁵. L'apposizione del referimento temporale prima della firma digitale trae

²⁶² il formato pdf/Archive è un nuovo formato della Adobe System Incorporated che garantisce a lungo termine la conservazione dei documenti elettronici.

²⁶³ D.M. 23/1/2004 art. 3 c. 1 lett. a) e b) : 1.I documenti rilevanti ai fini tributari:

a) hanno la forma di documenti statici non modificabili;

b) sono emessi, al fine di garantirne l'attestazione della data, l'autenticità, l'integrità, con l'apposizione del referimento temporale e della sottoscrizione elettronica

²⁶⁴ *Riferimento temporale*, informazione contenente la data e l'ora che viene associata ad uno o più documenti informatici; a differenza della marca temporale il referimento temporale è opponibile a terzi a discrezione del giudice. La sincronizzazione dei sistemi di apposizione del referimento temporale avviene tramite l'utilizzo di particolari software che tramite internet permettono di sincronizzare l'orologio del sistema con i NPT server web (Network Time Protocol) in grado di certificare con precisione data e ora. L'Istituto Elettrotecnico Galileo Ferraris fornisce un servizio di sincronizzazione per sistemi informatici collegati ad Internet usufruibile previa installazione di appositi software liberamente scaricabili.

²⁶⁵ *Firma digitale*, particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici(art. 1 lett. i) DMEF 23/1/2004);

motivazione dalla necessità di cristallizzare ad una data certa il contenuto dei documenti memorizzati (e/o conservati) realizzando un “*file di chiusura*”.

Modalità di esibizione art. 3 c. 1 lett. c)

La terza caratteristica dei documenti informatici rilevanti ai fini tributari è quella relativa all’*esibizione* prevista alla lettera c) del comma 1 dell’art. 3 del D.M. 23/1/2004²⁶⁶ che però, a tal fine, si limita a richiamare esplicitamente la disciplina sull’esibizione stabilita dall’art. 6²⁶⁷ dello stesso decreto ovvero: i documenti devono essere resi leggibili ed a richiesta anche disponibili su supporto cartaceo ed informatico e possono essere esibiti anche per via telematica secondo modalità stabilite con provvedimenti delle Agenzie fiscali.

Anche le scritture contabili tenute informaticamente possono essere esibite secondo tali modalità.

Memorizzazione art. 3 c. 1 lett. d)

I documenti informatici rilevanti ai fini tributari sono *memorizzati* su qualsiasi supporto di cui sia garantita *la leggibilità* nel tempo assicurando *l’ordine cronologico* e *l’assenza di soluzione di continuità* per ciascun periodo di imposta.

La memorizzazione, che rappresenta la fase iniziale del processo di conservazione, **può essere eseguita attraverso il salvataggio dei dati su supporto ottico o su ogni altro idoneo supporto.**

In merito all’**ordine cronologico** richiesto, esso riflette una memorizzazione dei documenti conforme con le tradizionali modalità di registrazione previste per i documenti fiscali, basti pensare ad esempio alle fatture attive il cui ordine cronologico viene determinato in base alla *data di emissione* del “documento fattura”.

Per quanto riguarda la caratteristica della “**non soluzione di continuità**” essa richiama esplicitamente il *principio di omogeneità* dell’archivio che è necessario seguire per quel determinato *periodo di imposta* che si è deciso di archiviare con modalità digitale.

Relativamente al periodo di imposta questo non è univocamente determinato essendo diversamente stabilito dalla disciplina fiscale in relazione

²⁶⁶ D.M. 23/1/2004 art. 3 c. 1: documenti rilevanti ai fini tributari:

- a) hanno la forma di documenti statici non modificabili;
- b) sono emessi, al fine di garantirne l’attestazione della data, l’autenticità e l’integrità, con l’apposizione del riferimento temporale e della sottoscrizione elettronica;
- c) sono esibiti secondo le modalità di cui all’art. 6;
- d) sono memorizzati su qualsiasi supporto di cui sia garantita la leggibilità nel tempo, purchè sia assicurato l’ordine cronologico e non vi sia soluzione di continuità per ciascun periodo d’imposta; inoltre, devono essere consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione al cognome, al nome, alla denominazione, al codice fiscale, alla partita Iva, alla data o associazioni logiche e questi ultimi.

²⁶⁷ Art. 6 D.M. 23/01/2004: 1. Il documento di cui all’art. 3 è reso leggibile e, a richiesta, disponibile su supporto cartaceo e informatico presso il luogo di conservazione delle scritture, in caso di verifiche, controlli o ispezioni.

2. Il documento conservato può essere esibito anche per via telematica secondo le modalità stabilite con provvedimenti dei direttori delle competenti Agenzie fiscali.

all'ambito cui sia attinente. Per le persone fisiche ad esempio esso viene individuato nell'anno solare (art. 7 DPR 917/1986²⁶⁸), per le società è rappresentato dall'esercizio o periodo di gestione della società determinato dalla legge o dall'atto costitutivo (art. 76 DPR 917/1986²⁶⁹).

Allo scopo, tra l'altro, di agevolare eventuali attività di controllo delle autorità fiscali, la memorizzazione dei documenti informatici rilevanti ai fini tributari deve essere predisposta in modo da consentire le *funzioni di estrapolazione* dei documenti archiviati mediante le seguenti chiavi di ricerca:

- *cognome*,
- *nome*;
- *denominazione*;
- *codice fiscale*;
- *partita iva*;
- *data*;
- *associazioni logiche di questi ultimi*.

Anche le scritture contabili, adempiendo ai predetti obblighi, possono essere memorizzate secondo la prevista normativa.

7. Il processo di conservazione sostitutiva dei documenti informatici rilevanti ai fini tributari

Il *processo di conservazione* dei documenti informatici genericamente intesi, il cui fine essenziale è, come già detto, quello di rendere documenti informatici e/o analogici in formato autentico non deteriorabili e disponibili per tutto il tempo per cui è richiesta la conservazione, è disciplinato in primo luogo dalla delibera CNIPA del 19 febbraio 2004 che si occupa appunto di stabilire "le regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali".

Nel caso del processo di conservazione dei documenti informatici rilevanti ai fini tributari *le disposizioni della delibera si intersecano con quelle previste dal D.M. 23 gennaio 2004.*

In particolare *l'articolo 3 del DMEF*, dopo aver elencato al comma 1 le caratteristiche richieste ai documenti informatici rilevanti ai fini delle disposizioni tributarie, al *comma 2*²⁷⁰ stabilisce che *la conservazione dei*

²⁶⁸ Art. 7 c. 1 DPR 917/1986 L'imposta è dovuta per anni solari, a ciascuno dei quali corrisponde un'obbligazione tributaria autonoma, salvo quanto stabilito nel comma 3 dell'art. 8 e nel secondo periodo del comma 3 dell'art. 12.

²⁶⁹ Art. 76 DPR 917/1986 L'imposta è dovuta per periodi di imposta, a ciascuno dei quali corrisponde una obbligazione tributaria autonoma salvo quanto stabilito negli articoli 80 e 84. Il periodo di imposta è costituito dall'esercizio o periodo di gestione della società o dell'ente, determinato dalla legge o dall'atto costitutivo. Se la durata dell'esercizio o periodo di gestione non è determinata dalla legge o dall'atto costitutivo, o è determinata in due o più anni, il periodo di imposta è costituito dall'anno solare.

²⁷⁰ art. 3 comma 2 D.M. 23 gennaio 2004 - Il processo di conservazione dei documenti informatici avviene mediante le modalità di memorizzazione previste al comma 1, lettera d), e secondo il procedimento indicato nell'art. 3 della deliberazione AIPA n. 42 del 2001 e termina con la

documenti in argomento *si svolge attraverso le modalità di memorizzazione di cui al* (già illustrato) *comma 1 lett. d) e secondo il procedimento previsto dall'art. 3 della delibera Cnipa n. 11 del 19 febbraio 2004*²⁷¹.

Per le caratteristiche dei documenti rilevanti ai fini tributari e per la memorizzazione vale, quindi, quanto esposto al paragrafo precedente.

Completata la fase di memorizzazione dei documenti, *il processo di conservazione termina con la sottoscrizione elettronica e l'apposizione della marca temporale*²⁷² *da parte del Responsabile della conservazione*²⁷³ *sull'insieme dei documenti, su una unica impronta*²⁷⁴ *dei documenti o su più impronte che rappresentino i singoli documenti o insiemi di essi.*

Da notare come l'apposizione della marca temporale consenta di avere la certezza, opponibile ai terzi, che il procedimento è stato portato a termine in data ed ora determinate.

Il c. 2 ultima parte l'art. 3 del DMEF detta la cadenza temporale con cui deve essere effettuato il processo di conservazione: *quindicinale* per le fatture e almeno *annuale* per i restanti documenti.

La conservazione realizzata seguendo le descritte modalità produce un effetto sostitutivo dei documenti conservati ed è quindi anche definita “*conservazione sostitutiva*”.

8. Il riversamento e l'esibizione dei documenti informatici rilevanti ai fini tributari.

I documenti informatici e/o analogici, dopo essere stati sottoposti a conservazione sostitutiva, possono essere sottoposti ad un processo di trasferimento, denominato “*riversamento*”, del loro contenuto da un supporto ottico a diverso supporto di tipo informatico.

Un tale procedimento può ritenersi necessario per fronteggiare talune evenienze quali, ad esempio, quella di esibire dei documenti mantenuti all'interno del sistema di conservazione.

Come indicato al comma 1, lettere o) e p) dell'art. 1 della deliberazione Cnipa n. 11/2004, il riversamento può essere *diretto* o *sostitutivo*.

Si parla di *riversamento diretto* quando il trasferimento del documento

sottoscrizione elettronica e l'apposizione della marca temporale, in luogo del riferimento temporale, sull'insieme dei predetti documenti o di insiemi di essi da parte del Responsabile della conservazione di cui alla deliberazione AIPA n. 42 del 2001. Il processo di conservazione è effettuato con cadenza almeno quindicinale per le fatture e almeno annuale per i restanti documenti.

²⁷¹ letteralmente l'art. 3 del D.M. cita la deliberazione AIPA n. 42 del 2001 sostituita integralmente dalla delibera Cnipa 11/2004

²⁷² *marca temporale*: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale D.M. 23 gennaio 2004 art. c. 1 lett. q)

²⁷³ *Responsabile della conservazione* definizione art. 5 della Deliberazione Cnipa 19 febbraio 2004: vedi pag. 21.

²⁷⁴ D.M. 23/1/2004 art. 1 c. 1 lett. m) *impronta*: sequenza di simboli binari (bit) di lunghezza predefinita generate mediante l'applicazione alla prima sequenza di un'opportuna funzione di hash. Attraverso una opportuna funzione matematica di un qualsiasi documento informatico viene estratta una sequenza di simboli binari ovvero “un'impronta” che lo identifichi in modo univoco e senza che dalla stessa sequenza sia possibile risalire al documento di origine.

conservato da uno ad altro supporto si verifica senza alterazione della sua rappresentazione digitale (ad esempio per la produzione di copie di sicurezza di un archivio). I documenti riversati vengono duplicati nel supporto di destinazione congiuntamente ai loro contrassegni di autenticità ovvero firme digitali, marche temporali, impronte ecc..

Nel *riversamento diretto*, proprio per il fatto che non si produce alcuna alterazione della rappresentazione informatica dei documenti, non sono previste “particolari modalità operative” e i documenti riversati conservano il valore di quelli da cui traggono origine.

Si realizza il *riversamento sostitutivo* quando il trasferimento di un documento conservato da uno ad altro supporto di memorizzazione comporti la modifica della rappresentazione informatica dei documenti.

Nel *riversamento sostitutivo*, pur restando inalterato il contenuto, si producono modifiche nella forma del documento che può passare ad esempio dal formato Pdf a quello Xml: questa procedura necessita quindi, a seconda del documento riversato, dell’ intervento del responsabile della conservazione o anche del pubblico ufficiale²⁷⁵.

In particolare, relativamente al riversamento sostitutivo, i *documenti informatici sottoscritti* ai sensi dell’articolo 10, commi 2 e 3 del D.P.R. 28 dicembre 2000, n. 445 così come modificato dall’articolo 6 del decreto legislativo 23 gennaio, n. 10, sono stati assimilati a quelli *digitali generati da analogici originali unici e*, per entrambe le suddette tipologie, diversamente a quanto previsto per la generalità dei documenti, è richiesto non solo l’intervento del responsabile della conservazione ma anche quello del pubblico ufficiale.

Il riversamento sostitutivo termina con l’apposizione della firma elettronica qualificata e della marca temporale sull’insieme dei documenti, ovvero su un’evidenza informatica contenete l’impronta o le impronte dei documenti o di insiemi di essi, da parte del solo responsabile della conservazione. Nel caso si tratti di documenti afferenti alle due tipologie “particolari” sopra indicate, è prevista l’ulteriore apposizione della sottoscrizione elettronica e del riferimento temporale da parte del pubblico ufficiale.

Si realizza sempre un riversamento sostitutivo quando un documento viene estrapolato dall’insieme dei documenti di un archivio informatico che era stato *oggetto* del processo di conservazione e *misura* per la generazione delle firme digitali richieste.

In particolare, il riversamento sostitutivo “consente l’aggiornamento

²⁷⁵ Art. 3 comma 2 delibera Cnipa n. 11/2004 – Conservazione sostitutiva di documenti informatici : Il processo di riversamento sostitutivo di documenti informatici conservati avviene mediante memorizzazione su altro supporto ottico e termina con l’apposizione sull’insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo. Qualora il processo riguardi documenti informatici sottoscritti, così come individuati nell’art. 1, lettera f), è inoltre richiesta l’apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d’origine.

tecnologico dell'archivio quando non sia possibile o conveniente mantenere nel tempo il formato della rappresentazione informatica dei documenti"²⁷⁶, *l'operazione si rende necessaria per adempiere l'obbligo di esibizione dei documenti.*

Nel caso di esibizione dei documenti informatici rilevanti ai fini tributari, ai sensi del combinato disposto dell'art. 6²⁷⁷ del DMEF e dell'art. 6 della Deliberazione Cnipa, il documento conservato su supporto informatico deve essere reso leggibile e, a richiesta, disponibile su carta o su supporto informatico presso il luogo di conservazione delle scritture contabili.

Naturalmente l'esibizione delle scritture contabili e dei documenti rilevanti ai fini tributari di cui all'art. 6 del DMEF è quella connessa alle attività di ispezione documentale tipiche degli organi di controllo dell'amministrazione finanziaria che, nell'ambito di loro competenza, possono appunto richiedere l'invio o l'esibizione di documenti.

Secondo quanto disposto dal comma 2 dell'art. 6 del DMEF è *consentita l'esibizione del documento conservato anche per via telematica* con modalità da stabilirsi con provvedimento del Direttore dell'Agenzia delle Entrate.

9. Tenuta delle scritture contabili con modalità informatiche

Anche per le *scritture contabili* tenute con modalità informatiche, che pure rivestono il carattere di documenti informatici rilevanti ai fini tributari, la norma di riferimento è l'art. 3 del D.M. 23 gennaio 2004, quindi, anche registri e libri tenuti digitalmente devono essere caratterizzati da quelle peculiarità di "*forma*", "*emissione*", "*esibizione*" e "*memorizzazione*" già analizzate.

In particolare, riguardo alla forma le scritture contabili devono essere formate come documenti statici non modificabili (Pdf ecc.) mentre relativamente all'emissione le stesse scritture devono essere rese autentiche ed integre attraverso l'apposizione del riferimento temporale e della firma digitale.

A proposito del termine "*emissione*" questo, in riferimento alle scritture contabili, non è da intendersi esclusivamente in senso stretto come il momento di "uscita" dalla sfera di disponibilità di chi le emette (come avviene ad es. per documenti quali le fatture) bensì nel senso di "*formazione definitiva*" così da considerare le scritture contabili "*emesse*" nel momento dell'apposizione del riferimento temporale e della firma digitale alle registrazioni eseguite.

I libri così *formati* ed *emessi* sono *esibiti* secondo le modalità di cui all'art. 6 del DMEF ovvero sono resi *leggibili* e, a richiesta *disponibili* su

²⁷⁶ Deliberazione Cnipa n. 11/2004 - Note esplicative delle regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico n. 6);

²⁷⁷ art. 6 D.M. 23/1/2004 : 1. Il documento di cui all'art. 3 è reso leggibile e, a richiesta, disponibile su supporto cartaceo e informatico presso il luogo di conservazione delle scritture, in caso di verifiche, controllino ispezioni. 2. Il documento conservato può essere esibito anche per via telematica secondo le modalità stabilite con provvedimenti dei direttori delle competenti Agenzie fiscali.

supporto cartaceo e informatico (art. 6 comma 1) *nonché per via telematica* (art. 6 comma 2).

Le scritture contabili sono infine *memorizzate* su un qualsiasi supporto di cui sia garantita la leggibilità nel tempo e nel rispetto dell'ordine cronologico e della continuità per ciascun periodo di imposta, requisiti, questi ultimi, richiesti espressamente dall'art. 3 del DMEF e più in generale previsti per i documenti informatici dalla normativa fiscale e civilistica.

Per il principio di continuità nel corso di uno stesso periodo d'imposta non sarà quindi possibile ad es. migrare da una tenuta della contabilità con modalità informatiche ad una contabilità su supporto cartaceo dovendosi attendere per mutare le modalità di tenuta delle scritture il successivo periodo di imposta.

Le modalità di memorizzazione impiegate devono permettere di eseguire estrapolazioni dei dati contenuti sulla base di predisposti "*campi di ricerca*".

Per le scritture contabili "*chiavi di ricerca*" possono ad esempio catalogarsi in : "*tipologia del libro*" (libro giornale, libro degli acquisti ecc.), "*anno di riferimento*", se il libro viene formato con cadenza inferiore a quella annuale anche con "*periodo di riferimento*".

La tenuta delle scritture contabili con modalità informatiche è sovrapponibile alla tenuta cartacea ove al concetto di "*stampa*" si sostituisca quello di "*formazione definitiva*".

10. Conservazione delle scritture contabili con modalità informatiche.

Si osserva preliminarmente che tenere le scritture contabili con modalità informatiche non obbliga il soggetto, l'impresa, l'azienda ecc., ad adottare per questi documenti una conservazione in formato digitale, ben potendo optare per la stampa dei registri in formato cartaceo entro i termini indicati per la presentazione delle dichiarazioni dei redditi conservando tale documentazione cartacea per dieci anni dall'ultima registrazione come stabilito dalle norme civilistiche.

Ai fini fiscali le norme tributarie, relativamente ai tempi di conservazione, impongono che i registri e i documenti rilevanti ai fini IVA siano conservati per quattro anni (art. 39 c. 3 DPR 633/1972 e art. 22 c. 2 DPR 600/1973) con decorrenza dal 31 dicembre dell'anno successivo a quello in cui è stata presentata la dichiarazione annuale; si tenga però presente che in caso di accertamento fiscale il termine viene prorogato fino alla definizione dell'accertamento e quindi, in teoria, anche oltre i dieci anni previsti dalla normativa civilistica (art. 2220 c.c.).

Anche il procedimento per la conservazione delle scritture contabili, così come gli altri documenti informatici rilevanti ai fini delle disposizioni tributarie, è disciplinato dal già analizzato comma 2 dell'art. 3 del D.M. 23 gennaio 2004 e dunque, *per sottoporre a conservazione digitale i libri contabili definitivamente formati e memorizzati su supporto, è necessario*

procedere all'apposizione della marca temporale²⁷⁸ e della firma digitale²⁷⁹ da parte del responsabile della conservazione sull'intero file o sull'evidenza informatica²⁸⁰ oggetto della conservazione contenente l'impronta²⁸¹.

Come già accennato in precedenza il processo di conservazione delle scritture contabili in formato digitale è effettuato con cadenza almeno annuale, essendo espressamente prevista dalla normativa una più stringente cadenza quindicinale esclusivamente per la conservazione delle fatture²⁸².

Il Decreto 23/1/2004 non indica quale sia il termine ultimo entro il quale debba concludersi il processo di conservazione delle scritture contabili ma, trattandosi di documenti sottoposti per definizione ad aggiornamento periodico, si ritiene che essi debbano risultare statici ed imm modificabili soltanto alla data in cui, in base a quanto previsto dalla normativa fiscale, non possano più eseguirsi registrazioni. A tale proposito, considerato che l'art. 7, comma 4-ter del D.L. 10/6/1994 n. 357 (convertito con modificazioni dalla legge 489/94) autorizza la tenuta di qualsiasi registro contabile con sistemi meccanografici, anche in difetto di trascrizione su supporti cartacei, a condizione che i dati registrati ma non ancora trascritti siano relativi "all'esercizio per il quale non siano scaduti i termini per la presentazione delle relative dichiarazioni annuali", si deduce che anche *i libri ed i registri tenuti con modalità digitali devono rivestire i caratteri di staticità ed imm modificabilità entro la data di scadenza delle dichiarazioni annuali cui si riferiscono i dati registrati.*

Da notare come, nel caso di controlli e/o ispezioni da parte dell'Amministrazione Finanziaria, il termine per concludere il procedimento di conservazione digitale dei documenti informatici debba venire anticipato rispetto alla normale cadenza prevista dalla norma e, registri e libri contabili debbano essere resi statici e non modificabili dall'inizio dell'anno alla data della disposta verifica²⁸³.

²⁷⁸ marca temporale: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale D.M. 23 gennaio 2004 art. 1 c. 1 lett. q)

²⁷⁹ firma digitale: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici D.M. 23 gennaio 2004 art. c. 1 lett. i)

²⁸⁰ evidenza informatica : sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica D.M. 23 gennaio 2004 art. c. 1 lett. o)

²⁸¹ impronta: sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima sequenza di un'opportuna funzione di hash D.M. 23 gennaio 2004 art. c. 1 lett. m)

²⁸² art. 3 comma 2 D.M. 23 gennaio 2004 - Il processo di conservazione dei documenti informatici avviene mediante le modalità di memorizzazione previste al comma 1, lettera d), e secondo il procedimento indicato nell'art. 3 della deliberazione AIPA n. 42 del 2001 e termina con la sottoscrizione elettronica e l'apposizione della marca temporale, in luogo del riferimento temporale, sull'insieme dei predetti documenti o di insiemi di essi da parte del Responsabile della conservazione di cui alla deliberazione AIPA n. 42 del 2001. Il processo di conservazione è effettuato con cadenza almeno quindicinale per le fatture e almeno annuale per i restanti documenti.

²⁸³ Circolare n. 45/E, 19 ottobre 2005 punto n. 4.

11. La conservazione sostitutiva di scritture contabili stampate su supporto cartaceo

Le nuove regole dettate dal DMEF del 23 gennaio 2004 in materia di conservazione sostitutiva dei documenti rilevanti ai fini tributari permettono non solo, come già visto, di memorizzare direttamente i documenti informatici (art. 3 comma 2) ma anche di eliminare il supporto cartaceo di quelli analogici attraverso un procedimento di traslazione dei dati dal supporto cartaceo ad altro supporto di tipo digitale.

In particolare l'art. 4 al comma 1 stabilisce che *“il processo di conservazione di documenti e scritture analogici rilevanti ai fini tributari avviene mediante memorizzazione della relativa immagine secondo le modalità di cui all'art. 3, commi 1 e 2”* rinviando esplicitamente alle **medesime modalità previste per i documenti informatici** e illustrate alle pagine precedenti.

Sostanzialmente quindi il procedimento di conservazione di scritture contabili tenute in formato cartaceo è il medesimo di quello previsto per quelle tenute in formato digitale, tuttavia tre particolarità differenziano i due procedimenti:

- un procedimento di scansione prodromico alla memorizzazione dell'immagine prevista dalla norma;
- l'intervento del pubblico ufficiale nel caso si tratti di documenti originali unici;
- la mancata previsione dell'obbligo di osservare tempi determinati (infatti trattandosi di un processo il cui fine fondamentale è quello di smaterializzare un archivio analogico già esistente non è richiesta l'osservanza di termini specifici).

Relativamente al procedimento di scansione si segnala che generalmente si praticano due modalità di scansione dei documenti: tramite **ocr** (optical character recognition - riconoscimento ottico dei caratteri) e per **immagine**.

Nel primo caso il software individua e riconosce i caratteri presenti nel documento e li dispone in un *file di testo* utilizzabile da un qualsiasi editor visuale (es. Microsoft Word) ed a tale proposito, benchè la tecnologia attualmente permetta di ottenere ottimi risultati, bisogna dire che molto dipende dallo stato di conservazione del documento cartaceo originale, la qualità della sua stampa ecc. per cui spesso sono necessari piccoli interventi correttivi.

La scansione per immagine prevede, invece, la trasformazione del documento cartaceo in un *file di immagine*, pertanto viene sempre preservato il testo originale.

Per quanto riguarda le caratteristiche richieste dalla normativa, anche le scritture contabili in formato cartaceo (così come gli altri i documenti analogici) con il procedimento di conservazione ottica:

- assumono la forma di documenti statici non modificabili;

- sono memorizzati su un supporto ottico (e non) che ne garantisca nel tempo la leggibilità;

- concludono il processo di conservazione dopo l'apposizione della firma digitale e della marca temporale da parte del responsabile della conservazione (e in caso di documenti originali unici, anche da parte di un pubblico ufficiale). Secondo quanto disposto dall'art. 4 comma 4²⁸⁴ del DMEF successivamente al completamento della procedura di conservazione digitale è consentita la distruzione dei documenti analogici ovvero, caso che qui più interessa, dei libri contabili cartacei di origine.

12. Invio dell'impronta all'Amministrazione finanziaria

Concluso il procedimento di conservazione delle scritture contabili entro il termine stabilito per la presentazione delle dichiarazioni fiscali ulteriori adempimenti sono previsti dall'art. 5 comma 1²⁸⁵ del DMEF, detta norma infatti stabilisce che, entro il mese successivo alla scadenza dei termini per la presentazione delle dichiarazioni fiscali relative alle imposte sui redditi, all'imposta regionale sulle attività produttive e all'imposta sul valore aggiunto, il soggetto interessato o il responsabile del procedimento, ove designato, al fine di *estendere la validità dei documenti informatici trasmette alle competenti Agenzie fiscali l'impronta dell'archivio informatico* oggetto della conservazione, la relativa sottoscrizione elettronica e la marca temporale. Peraltro, come chiarito dalla Circolare 36/2006, attraverso la comunicazione si attribuisce specifica rilevanza fiscale ai documenti conservati secondo le regole del DMEF.

Con appositi provvedimenti da emanarsi, le Agenzie stesse potrebbero chiedere ulteriori dati ed elementi identificativi (art. 5 comma 2 DMEF). Secondo quanto previsto dal comma 3 dell'art. 5 del D.M. l'Agenzia renderà disponibile *“per via telematica la ricevuta della comunicazione effettuata ed il relativo numero di protocollo”*.

Il dettato normativo non prevede espressamente la necessità di trasmettere tutte le impronte generate nonché le sottoscrizioni e le marche apposte *periodicamente*²⁸⁶ sui documenti oggetto di conservazione, si ritiene quindi sufficiente generare dall'*intero archivio* un'unica impronta ovvero una *“super – impronta”*, univocamente riferibile al periodo d'imposta concluso,

²⁸⁴ Art 4 c. 4 del DM 23/1/2004 – La distruzione dei documenti analogici, di cui è obbligatoria la conservazione è consentita soltanto dopo il completamento della procedura di conservazione digitale.

²⁸⁵ art. 5 D.M. 23/1/2004 c. 1 Entro il mese successivo alla scadenza dei termini stabiliti dal decreto del Presidente della Repubblica n. 322 del 1998, per la presentazione delle dichiarazioni relative alle imposte sui redditi, all'imposta regionale sulle attività produttive e all'imposta sul valore aggiunto, il soggetto interessato o il responsabile della conservazione, ove designato, al fine di estendere la validità di documenti informatici trasmette alle competenti Agenzie fiscali, l'impronta dell'archivio informatico oggetto della conservazione, la relativa sottoscrizione elettronica e la marca temporale. **c. 2** Con provvedimento le Agenzie fiscali indicano gli ulteriori dati ed elementi identificativi da comunicare unitamente a quelli del precedente comma. **c. 3** Le stesse Agenzie rendono disponibile per via telematica la ricevuta della comunicazione effettuata ed il relativo numero di protocollo.

²⁸⁶ Si pensi al caso delle fatture elettroniche per cui è prevista una cadenza quindicinale.

accompagnata dalla relativa sottoscrizione elettronica e marca temporale.

Secondo quanto specificato dalla circolare 36/2006 è in corso di emanazione, da parte del Direttore dell'Agenzia delle Entrate, il provvedimento con cui saranno approvate le specifiche tecniche necessarie alla trasmissione telematica della *comunicazione* in esame.

Nel frattempo, i contribuenti non sono tenuti ad effettuare l'invio dell'impronta dell'archivio informatico oggetto della conservazione.

13. Esempi di procedimenti di conservazione di scritture contabili

Il procedimento di conservazione sostitutiva può essere attivato per tutte le scritture contabili tenute da un'azienda, impresa società ecc.; di seguito si riportano alcuni esempi circa le procedure da seguire per i libri più comuni quali il libro giornale e i registri iva.

Conservazione del Libro giornale (art. 2216 cc. – art.22 dpr 600/1973)

- **formazione** come documento informatico statico non modificabile almeno una volta l'anno, preferibilmente ogni 30/60 giorni con apposizione del riferimento temporale e della firma digitale prima della scadenza del termine per l'invio delle dichiarazioni fiscali;

- **conservazione** con modalità informatiche attraverso la produzione con cadenza annuale di una evidenza informatica che contenga le 12/6 impronte di hash, a seconda se i periodi di formazione adottati siano con cadenza mensile o bimestrale, ed apposizione della marca temporale e della firma digitale da parte del responsabile della conservazione.

Conservazione dei Registri iva:

Tra i registri previsti dalla normativa sull'imposta del valore aggiunto ai fini dell'annotazione cronologica delle operazioni rilevanti i più comuni ed importanti sono:

- il registro delle fatture emesse;
- il registro dei corrispettivi;
- il registro degli acquisti.

Per la conservazione dei registri iva si può procedere come segue:

- **formazione** come documento informatico statico non modificabile almeno una volta all'anno (o su base mensile o trimestrale al termine della liquidazione dell'iva) e apposizione della firma digitale e del riferimento temporale prima della scadenza del termine per l'invio delle dichiarazioni fiscali;

- **conservazione** attraverso la generazione annuale di una evidenza informatica che contenga l'impronta di hash relativa all'annualità in oggetto (o le 12 o 4 impronte di hash relative ai periodi infrannuali) ed apposizione da parte del responsabile della conservazione della marca temporale e della firma digitale.

Il processo di conservazione delle scritture contabili di cui sopra si

conclude con l'invio, entro il mese successivo alla scadenza dei termini utili per la presentazione delle dichiarazioni fiscali, dell'impronta dell'archivio informatico oggetto della conservazione all'Agenzia delle Entrate secondo quanto stabilito dall'art. 5 comma 1 del DM 23 gennaio 2004.

14. Il Responsabile della conservazione

La disciplina in materia di riproduzione e conservazione dei documenti in formato digitale, ha introdotto una nuova figura di fondamentale rilievo che sovrintende al corretto svolgimento delle procedure di conservazione e ne garantisce nel tempo le caratteristiche: *il responsabile della conservazione*.

La norma che stabilisce con puntualità compiti ed obblighi posti a carico del responsabile è l'art. 5 della deliberazione Cnipa n. 11 del 19 febbraio 2004 che ha sostituito integralmente il precedente art. 5 della delibera Aipa n. 42/2001 cui fa esplicito riferimento l'art. 3 comma 2²⁸⁷ del DMEF.

Al responsabile della conservazione sono demandati i compiti di :

- *Definire* le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare;
- *Organizzare* il contenuto dei supporti ottici e gestire le procedure di sicurezza e tracciabilità atte a garantire la corretta conservazione nonché l'esibizione dei documenti custoditi;
- *Mantenere* e rendere accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- *Verificare* la corretta funzionalità del sistema e dei programmi in gestione;
- *Adottare* le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
- *Richiedere* la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento ed assicurare l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- *Definire* e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- *Verificare* periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.
- *Archiviare* e rendere disponibili relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
 - descrizione del contenuto dell'insieme dei documenti;
 - estremi identificativi del responsabile della conservazione e/o dei soggetti eventualmente da questi delegati, con l'indicazione dei compiti agli stessi assegnati;

²⁸⁷ art. 3 comma 2 DM gennaio 2004: Il processo di conservazione dei documenti informatici avviene mediante...e termina con la sottoscrizione elettronica e l'apposizione della marca temporale ...da parte del responsabile della conservazione di cui all'art. 5 della deliberazione AIPA n. 42 del 2001..."

- indicazione delle copie di sicurezza.

Spetta al responsabile della conservazione, sulla base di una discrezionalità professionalmente orientata, terminare il processo di conservazione con la sottoscrizione elettronica e l'apposizione della marca temporale sull'insieme dei documenti, ovvero sull'unica impronta degli stessi, o su più impronte che rappresentino i singoli documenti o insiemi di essi.

Sintetizzando, compiti prioritari ed essenziali del responsabile della conservazione sostitutiva risultano essere:

- l'organizzazione, l'attivazione e aggiornamento tecnologico di un adeguato impianto di hardware e software;
- la pianificazione dell'intero sistema di conservazione e cioè le procedure concretamente adottabili al fine di realizzare un processo di conservazione che risulti aderente e conforme all'ordinamento fiscale;
- il periodico accertamento del regolare il funzionamento delle procedure di conservazione attivate;
- la stesura del manuale della conservazione sostitutiva in cui esporre l'architettura logica del sistema di conservazione informatico in uso e le procedure adottate come ad esempio le misure di sicurezza, lo schema di gestione dei documenti per tipologia, la struttura dell'archivio software e metodologia di accesso ai documenti;
- la verifica della corretta esecuzione del processo di conservazione, lo stato di conservazione ed efficienza dei supporti e l'effettiva leggibilità dei documenti;
- la predisposizione di idonee procedure finalizzate al tempestivo recupero dei documenti da esibire nel caso di richieste prodotte dall'Autorità fiscale.

Tra le attività, che pur non essendo tassativamente previste a suo carico dalla normativa di riferimento, si ritiene debbano essere svolte dal responsabile, si segnalano:

- la predisposizione ed aggiornamento del manuale della conservazione sostitutiva;
- la partecipazione ad eventuali accessi, ispezioni e verifiche da parte dell'Amministrazione Finanziaria, accadimenti nel corso dei quali si potrebbe prospettare la necessità di rendere disponibili su supporto cartaceo e/o informatico nonché di esibire documenti conservati;
- la produzione in via telematica all'Amministrazione Finanziaria dei documenti conservati.

I compiti demandati al Responsabile della conservazione risultano dunque essere molteplici e complessi ed esigono approfondite conoscenze non solo di tipo tecnico-informatico, ma anche giuridico-fiscale, non indipendenti da capacità di programmazione, pianificazione e controllo posto che il suo compito è, tra gli altri, anche quello di saper valutare i potenziali rischi dei processi organizzati ed introdurre le necessarie tutele.

Nella complessiva gestione dell'intero processo di conservazione dei

documenti rilevanti ai fini tributari egli dovrà rendersi garante, oltre che nei confronti dei soggetti per i quali svolge il suo lavoro, anche nei confronti dell'Amministrazione finanziaria di aver gestito la conservazione conformemente a principi di sicurezza stabiliti e documentati ed attraverso procedure di tracciabilità che assicurino la corretta conservazione, accessibilità ed esibizione di ogni documento.

E' di tutta evidenza che il ruolo del responsabile non si esaurisce nella pedissequa osservanza di una normativa dovendo egli operare anche attraverso procedure autonome, supporti scelti con professionalità e conformati alla realtà applicativa dell'ambiente nel cui ambito è chiamato ad intervenire dato che la sua azione deve tenere conto anche della tipologia dei documenti da conservare.

L'ordinamento non statuisce chi debba assumere un ruolo così autorevole e significativo ma il mancato formale incarico che individui il responsabile della conservazione priva di validità lo stesso processo.

L'investitura potrebbe essere assegnata sia ad un soggetto interno alla struttura interessata (dipendente, legale rappresentante ecc.) sia ad uno esterno alla medesima (commercialista, consulente fiscale ecc.) attraverso un formale atto di nomina.

Il secondo comma l'articolo 5²⁸⁸ della delibera CNIPA n. 11/2004 prevede che il responsabile possa delegare in *toto* o parzialmente lo svolgimento della propria attività ad una o più persone che per competenza ed esperienza garantiscano la corretta esecuzione delle operazioni ad esse affidate.

Il terzo comma dell'art. 5²⁸⁹ prevede infine che dell'intero procedimento di conservazione possa essere dato incarico, in tutto o in parte, a soggetti terzi, pubblici o privati anch'essi comunque tenuti ad osservare le disposizioni del DMEF e della delibera Cnipa n. 11/2004.

Questa ultima previsione si inquadra nella cosiddetta conservazione sostitutiva in *outsourcing*.

Occorre precisare che, nel caso la società, azienda, impresa ecc. opti per quest'ultima tipologia di conservazione, l'*outsourcer* non assume alcun tipo di responsabilità nei confronti dell'Autorità Finanziaria dovendo egli rispondere solo per responsabilità contrattuale ex art. 1218 c.c. al proprio committente che rimane unico responsabile ai fini fiscali.

15. L'intervento del pubblico ufficiale

²⁸⁸ Art. 5 comma 2 delibera Cnipa 11/2004: "Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione."

²⁸⁹ Art. 5 comma 3 delibera Cnipa 11/2004: "Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione."

Secondo quanto prescritto dall'art. 4 comma 1²⁹⁰ dalla delibera CNIPA n. 11/2004 il processo di conservazione sostitutiva dei documenti analogici originali, come pure dei documenti informatici, si conclude con le formalità dell'apposizione del riferimento temporale e della firma digitale da parte del Responsabile sull'insieme dei documenti destinati alla conservazione o su una evidenza informatica contenente una o più impronte dei documenti o insieme di essi.

Nel caso però di conservazione di *documenti informatici generati da documenti analogici originali unici* l'art. 4 comma 2²⁹¹ della Delibera impone che l'intervento del responsabile della conservazione venga necessariamente implementato da quello di un pubblico ufficiale.

Per pubblico ufficiale si intendono oltre al notaio, anche il cancelliere, il segretario comunale o incaricato del sindaco²⁹².

Finalità precipua dell'apposizione del riferimento temporale e della firma digitale da parte del pubblico ufficiale è quella di attestare la **conformità del documento conservato a quello di origine**.

Diversamente dalla delibera, il D.M. 23/1/2004 all'art. 4 comma 3²⁹³, a proposito del momento conclusivo della conservazione digitale dei documenti rilevanti ai fini tributari, non si è preoccupato di distinguere tra documenti analogici originali unici e non unici dando così origine a gravi dubbi interpretativi circa l'includibilità dell'intervento del pubblico ufficiale. Da qui la necessità di un intervento chiarificatore finalizzato a sciogliere le incertezze insinuate alla norma: la mancata limitazione *expressis verbis* dell'intervento del pubblico ufficiale ai soli documenti analogici unici era dovuta ad una consapevole scelta del legislatore fiscale o non era piuttosto frutto di una sua involontaria dimenticanza di inserimento del termine "*unici*"?

La problematica, come si intuisce di non poco conto, è stata chiarita dalla Circolare n. 36 dell'Agenzia delle Entrate che al punto 8.3 recita: "...il pubblico ufficiale deve obbligatoriamente partecipare al processo di:

1. conservazione elettronica di documenti *originali unici* ai sensi

²⁹⁰ Art. 4 comma 1 della delibera CNIPA n. 11/2004: "Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente su supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del Responsabile della conservazione che attesta così il corretto svolgimento del processo.

²⁹¹ Art. 4 comma 2 della delibera CNIPA n. 11/2004: "Il processo di conservazione sostitutiva di documenti analogici unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine".

²⁹² Art. 5 c. 4 Deliberazione CNIPA n. 11/2004: "Nelle amministrazioni pubbliche il ruolo di pubblico ufficiale è svolto dal dirigente dell'ufficio Responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per quanto previsto dall'articolo 3, c. 2 e dall'articolo 4, commi 2 e 4, casi nei quali si richiede l'intervento di un soggetto diverso della stessa amministrazione.

²⁹³ D.M. 23/1/2004 art. 4 comma 3. Il processo di conservazione digitale di documenti analogici originali avviene secondo le modalità di cui al comma 1 e si conclude con l'ulteriore apposizione del riferimento temporale e della sottoscrizione elettronica da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.

dell'articolo 4 della delibera CNIPA;

2. riversamento sostitutivo di documenti analogici *originali unici*, ai sensi dell'articolo 4 della delibera CNIPA;

3. riversamento sostitutivo dei documenti informatici sottoscritti, ai sensi dell'articolo 3 del decreto e dell'articolo 3 della delibera CNIPA. “.

Nel caso si sia proceduto a conservare informaticamente documenti unici, l'Amministrazione finanziaria potrebbe procedere ad interventi finalizzati ad accertare l'avvenuta osservanza dell'adempimento di richiesta dell'intervento del pubblico ufficiale.

Qualora nei casi previsti non si ottemperi a richiedere l'intervento del pubblico ufficiale, si ritiene non possa procedersi alla distruzione dei documenti analogici e qualora lo si faccia i documenti conservati possano essere ritenuti invalidi, ciò non solo ai fini fiscali ma anche in ambito civilistico nei casi in cui l'intervento del pubblico ufficiale sia previsto come condizione necessaria del procedimento di conservazione dei documenti ai fini civilistici (Deliberazione CNIPA del 19 febbraio 2004).”.

16. Manuale della conservazione

Tra gli obblighi previsti dalla normativa nel corso del processo di conservazione sostituiva dei documenti informatici rilevanti ai fini tributari, non è compreso quello della tenuta del manuale della conservazione eppure è innegabile che tale strumento sia da ritenersi di essenziale ausilio ai fini organizzativi e procedurali sia per il responsabile della conservazione sia per la stessa impresa, azienda ecc. che abbia deciso di aderire alla conservazione dei documenti secondo le introdotte modalità digitali.

Il manuale si configura come un documento interno in cui vanno riportati tutti i dati identificativi della struttura, del responsabile della conservazione e di coloro da questi eventualmente delegati.

Al suo interno vanno altresì riportati, nel dettaglio operativo, tutti i dati necessari alla comprensione di come sia strutturato l'intero processo di conservazione, compresi i moduli di implementazione ed aggiornamento. Nel manuale, che necessariamente deve essere integrato con altri documenti aziendali già in uso come il Documento programmatico della sicurezza, è inoltre utile indicare tutti gli adempimenti posti in essere in osservanza degli obblighi di legge.

In particolare il manuale della conservazione non deve tralasciare di archiviare e contenere le impronte all'atto della loro generazione nonché descrivere:

- le competenze, i compiti e le responsabilità del Responsabile della conservazione sostitutiva dei documenti rilevanti ai fini tributari;
- il processo di apposizione di firma digitale, della marca temporale e gli aspetti procedurali relativi alla registrazione dei dispositivi ottici sostitutivi;
- le procedure di sicurezza adottate per il processo di conservazione

sostitutiva e le procedure manutentive;

- lo schema di gestione dei documenti per tipologia;
- la metodologia di accesso ai documenti;
- le misure per la sicurezza fisica e logica;
- le misure adottate in materia di dati personali;
- le modalità di assolvimento dell'imposta di bollo;
- le procedure previste per la gestione di eventi catastrofici.

Nel manuale è inoltre opportuno vengano indicati il modo in cui è stato implementato il processo di conservazione e gli aspetti operativi che hanno contribuito alla produzione del dispositivo ottico contenete la documentazione digitale.

Il manuale della conservazione può essere sostituito da appropriati programmi di gestione documentale che dispongono di un particolare catalogo: le funzioni di work-flow di tali programmi richiamano con puntualità le scadenze delle diverse attività mentre le funzioni di monitoraggio registrano ogni singola operazione eseguita in un elenco cronologico utile, tra l'altro, per ricostruire fatti e responsabilità.

17. I supporti per la conservazione sostitutiva in formato digitale

I processi conservativi dei documenti sono in genere sostanzialmente finalizzati ad assicurare una idonea fruibilità nel tempo di quanto conservato ma nel processo di conservazione sostitutiva occorre soddisfare, in particolare, due fondamentali esigenze che rappresentano sinteticamente il motivo stesso del processo:

- la prima esigenza è quella della garanzia che quanto conservato corrisponda perfettamente all'originale e non subisca nel tempo alterazioni né accidentali né fraudolente;

- la seconda esigenza, non meno importante della precedente, è che i documenti trasferiti sugli appositi supporti al fine di essere conservati siano leggibili per tutto il tempo per cui è richiesta la conservazione.

Nello specifico, l'esigenza di avere la sicurezza che il documento conservato sia identico all'originale è garantita dal responsabile della conservazione attraverso l'apposizione della firma digitale e della marca temporale (adempimenti eventualmente implementati dall'intervento del pubblico ufficiale nel caso si tratti di documenti analogici unici), nonché attraverso il prolungamento dell'efficacia delle firme prima della scadenza del relativo certificato.

La risposta all'esigenza di assicurare nel tempo la leggibilità dei documenti conservati viene fornita dall'impiego di supporti basati su tecnologia laser (CD, DVD ecc.), dall'assolvimento dell'obbligo di produrre copie di sicurezza e da quello di verificare periodicamente, con cadenza almeno quinquennale, l'effettiva leggibilità dei documenti conservati.

Da notare che la Deliberazione Cnipa 11/2004, mentre agli articoli 3 e 4 fa esplicito riferimento ai “*supporti ottici*”, all'articolo 8 dà facoltà, ove non

ostino particolari motivazioni, di utilizzare “...qualsiasi supporto di memorizzazione, anche non ottico...”.

Al punto 4. delle note esplicative che accompagnano le regole tecniche dettate dal Cnipa si conferma l’autorizzazione ad utilizzare “qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser; quindi non soltanto dischi ottici Worm e CD-R, ma anche magneto- ottici e DVD...”

Il Decreto del Ministro dell’Economia e delle Finanze del 23 gennaio 2004 fa invece esplicito riferimento ad un processo di memorizzazione da effettuarsi “su qualsiasi supporto di cui sia garantita la leggibilità nel tempo”²⁹⁴.

Ciò sembrerebbe indicare come, a parere del Ministero delle Finanze, non sia poi così importante, nel il processo di conservazione dei documenti rilevanti ai fini tributari, il supporto che viene utilizzato posto che unica preoccupazione formalmente espressa risulta essere quella di garantire nel tempo la leggibilità e l’esibizione di documenti che, in caso contrario, si configurerebbero come non disponibili presso i contribuenti.

In conclusione dunque la normativa non impone nel processo di conservazione sostitutiva l’adozione di supporti a tecnologia laser anche se, dal punto di vista tecnico essi risultino attualmente i più vantaggiosi e ciò per un duplice ordine di motivi: perché in grado di assicurare una più lunga durata e perchè, trattandosi di elementi trasferibili, consentono una “migliore distribuzione geografica delle copie generate a maggior garanzia delle possibilità di *recovery* di quanto registrato”

Tra le tecnologie attualmente più in uso figurano i Dischi ottici, DVD ed i compact disk , CD.

I supporti dotati di tecnologia laser non risultano influenzati da campi magnetici ed hanno una durata molto estesa, ad esempio per i Dischi ottici UDO (ultra density optical) da 5,25 e 12 pollici c’è una previsione di durata rispettivamente di cinquanta e cento anni.

Per quanto riguarda supporti come i CD c’è da rilevare come essi, non essendo protetti da cartucce, rappresentino la tecnologia meno resistente e quindi meno stabile nel tempo, motivo questo forse che ha influenzato il legislatore nell’istituire tra gli obblighi previsti nel processo di conservazione sostitutiva quello di verificare periodicamente l’effettiva leggibilità dei documenti conservati²⁹⁵.

In ogni caso le odierne tecnologie, in particolare quelle Raid per i dischi magnetici, le procedure di retention e refresh dei nastri, nonché le procedure di back-up e disaster- recovery, fanno sì che le probabilità di perdere informazioni, specie se registrate su supporti di qualità connessi a

²⁹⁴ D.M. 23/1/2004 – art 3, c. 1 “...I documenti informatici rilevanti ai fini tributari...sono memorizzati su qualsiasi supporto di cui sia garantita la leggibilità nel tempo...”.

²⁹⁵ Delibera cnipa 11/2004 – art. 5 “ Il Responsabile del procedimento di conservazione sostitutiva ...verifica periodicamente, con cadenza non superiore a cinque anni, l’effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti...”.

idonei software di gestione, siano da considerarsi assai scarse.

Un buon Sistema di Conservazione Sostitutiva può realizzarsi attraverso supporti “rimovibili” che possono trovare una apposita e magari a sé stante collocazione negli spazi aziendali o dell’ufficio in ragione delle più modeste ipotesi di consultazione.

Ulteriori esigenze, da tenere presenti quando si parla di conservazione documentale in formato digitale e da associare alle due indicate in precedenza, sono quella relativa alla necessità di adottare tutte le misure atte a scongiurare che durante la fase di conservazione non vengano erroneamente sovrascritte registrazioni eseguite in precedenza nonché quella concernente la collocazione dei documenti conservati che, magari siti all’interno di un apposito archivio di conservazione, debbono risultare di facile reperibilità. Mentre la prima richiesta può ritenersi soddisfatta dall’impiego di supporti di registrazione Worm (write once read many), per la seconda pare opportuno organizzare un apposito indice dei documenti conservati ed installare una procedura che in caso di perdita ne consenta la ricostruzione.

18. Conclusioni

Ad oltre dieci anni dall’emanazione dell’art. 7 bis della legge 357/94 con cui veniva introdotta dall’ordinamento la possibilità di conservare scritture e documenti contabili sotto forma di registrazioni su supporti di immagine e ad oltre due anni dalla disciplina introdotta dal DMEF del 13/1/2004 e dalla Deliberazione Cnipa 11/2004, si può sostenere come il processo di conservazione sostitutiva sia una realtà già avviata per talune strutture aziendali che, prima di altre, hanno saputo cogliere le potenzialità di economia, sviluppo ed efficienza connesse all’adozione di un tale innovativo procedimento.

Non vi è dubbio che la concreta ed operativa adesione alla cultura dell’innovazione digitale possa implicare, nell’immediato, il sostenimento di costi non indifferenti per la necessaria reingegnerizzazione dei processi a carico di Privati e Pubblica Amministrazione.

Nè si possono inoltre ignorare, tra le altre difficoltà insite nella ricerca del superamento di una concezione di archiviazione e conservazione dei documenti collegata a sovrabbondanti ma pur sempre tradizionalmente rassicuranti archivi fisici; eppure, il fatto che l’uso delle tecnologie informatiche goda ormai del riconoscimento dell’ordinamento, e che strumenti ad esempio quali il documento informatico e la fattura elettronica, anche ai fini fiscali, abbiano anch’essi ricevuto il riconoscimento di una piena validità ai fini legali, costituisce una concreta e significativa opportunità di crescita e di sviluppo della odierna società della dell’informazione e della comunicazione tecnologica che è necessario cogliere al più presto.

CAPITOLO XIII

RAFFAELE MONTANARO

INFORMATIZZAZIONE DEL SISTEMA NORMATIVO IN AMBITO
PUBBLICO E NUOVE TECNOLOGIE

SOMMARIO: 1. Introduzione. – 2. Il processo di informatizzazione del *corpus* normativo attraverso le disposizioni emanate. – 3. Analisi del processo tecnico di informatizzazione degli atti normativi, la rappresentazione informatica del testo normativo: problemi e procedure. – 4. L'informatizzazione come occasione per il riordino e la semplificazione del corpus normativo. – 5. Conclusioni. – 6. Allegato n. 1. – 7. Allegato n. 2.

1. Introduzione.

Lo sviluppo delle nuove tecnologie informatiche costituisce una importante opportunità per rendere più accessibile, tanto ai cittadini quanto agli operatori, la conoscenza delle disposizioni e delle norme che regolamentano la vita della società italiana.

Attualmente, l'accessibilità è resa difficile dalla complessità di una normativa estremamente stratificata, nella quale si intrecciano vari piani e competenze, rimandi e abrogazioni - non sempre espliciti - che rendono difficoltosa sia la ricerca e la verifica delle norme vigenti, sia la loro interpretazione e applicazione.”²⁹⁶

Inoltre, il linguaggio usato nella redazione delle norme, è sovente farraginoso e non facilmente comprensibile al contrario la chiarezza del testo legislativo, chiarezza della struttura testuale e chiarezza del linguaggio utilizzato, è condizione essenziale della sua comprensibilità e applicabilità.

Ciò spiega quanto sia essenziale potersi riferire a basi documentali affidabili e complete. Per rendersi conto di quanto questa esigenza sia sentita, soprattutto dagli operatori del diritto, è sufficiente constatare la rilevanza economica del segmento di mercato relativo all'editoria giuridica in formato elettronico.²⁹⁷

Alcuni soggetti istituzionali, consapevoli dell'importanza di offrire ai cittadini l'accesso alla conoscenza degli atti normativi hanno messo le basi per la realizzazione di un sistema informatico nel quale fosse possibile /reperire la documentazione di carattere normativo emanata dai diversi soggetti pubblici,

²⁹⁶ Queste tematiche vengono ampiamente analizzate da vari autori, vedi, in particolare: R. Pagano, "Introduzione alla legistica", Giuffrè, 2004; V. Di Ciolo, "La progettazione legislativa in Italia, Giuffrè 2002 e M. Ainis, "La legge oscura", Laterza, 2002.

²⁹⁷ Appare significativo il fatto che oggi esistono undici operatori in grado di offrire accesso a banche dati giuridiche: due di questi sono soggetti pubblici, gli altri nove sono privati, di cui otto già presenti sul mercato, il cui valore complessivo è stato stimato, per il solo 2004, tra i 200.000.000 e i 300.000.000 di euro. Cfr. Autorità garante della concorrenza e del mercato, Bollettino 8/2005.

affrontando al tempo stesso il dilemma (a cui hanno dato una risposta positiva) circa la gratuità di tali risorse²⁹⁸.

Questo progetto, denominato “Norme in rete” si è dato un duplice obiettivo:

- **Consentire la realizzazione di un servizio “al cittadino”:**
 - gratuito e libero;
 - semplice da utilizzare;
 - che consenta una maggiore efficacia nelle ricerche;
- **Sperimentare una modalità di cooperazione tra diverse Amministrazioni,**²⁹⁹

Vediamo di ripercorrere l’iter che, partendo dal contratto stipulato il 14 maggio 1999 fra il Ministero della Giustizia e l’Istituto per la documentazione giuridica del CNR (IDG) per la realizzazione di uno Studio di fattibilità concernente la realizzazione di un sito-guida Web per l’”Accesso alle norme in rete ha portato allo sviluppo di questo progetto con la realizzazione del sito www.nir.it (che costituisce, oggi, un punto di accesso unitario per la ricerca su tutta la documentazione normativa pubblicata sul Web da organismi istituzionali), nonché allo sviluppo di ulteriori progetti di informatizzazione della normativa.³⁰⁰

2. Il processo di informatizzazione del *corpus* normativo attraverso le disposizioni emanate.

Il primo passo concreto verso una diffusa accessibilità alle fonti normative per via informatica è stato effettuato dal Ministero della Giustizia,³⁰¹ il quale nel 1999 promosse un progetto, la cui finalità era quella di “realizzare uno strumento unificato di accesso a tutte le fonti giuridiche, secondo le interfacce tipiche dei servizi Web [...]. I servizi progettati dovranno operare [...] al servizio del cittadino, ma anche di coloro che

²⁹⁸ “Come possiamo pretendere l’osservanza delle leggi quando le leggi per conoscerle le devi pagare? La P.A. si deve tirare indietro quando entra in competizione con il privato, perché il privato può fare un business del dato ricostruito, commentato e così via? Il problema di fondo che noi ora stiamo giusto affrontando con un progetto, finanziato anche dall’AIPA, che vede fra l’altro la partecipazione di alcune regioni riguarda la gratuità dell’accesso alla informazione giuridica.” Cfr. F. Roller, Convegno *Il patrimonio informativo della P.A. come servizio. I dati pubblici sono pubblici?* Forum PA 8 maggio 2000

²⁹⁹ Cfr. l’articolo di C. Lupo “Il progetto intersettoriale *Normeinrete*” in *Bollettino AIPA Informazioni*, Anno I nuova serie n. 11-12, Novembre-Dicembre 1999 reperibile all’indirizzo <http://www.normeinrete.it/stdoc/nirinbollettinoaipa.doc>

³⁰⁰ Per ulteriori approfondimenti vedi il numero monografico della Rivista Informatica e diritto, I, 2000, ESI Napoli

³⁰¹ In realtà, già verso la metà degli anni ’70 la Corte Suprema di Cassazione diede l’avvio ad un progetto di informatizzazione del dato normativo, (*Italgirefind*), il quale, però, essendo finalizzato ad agevolare il lavoro in primo luogo dei magistrati o comunque di ristrette categorie professionali, è stata (e, almeno per alcuni aspetti, ancora parzialmente è) una realtà fondamentale, ma circoscritta che non teneva in conto la fruibilità da parte dei cittadini.

operano nell'ambito della P.A. (in particolare presso gli uffici di gabinetto, gli uffici legislativi, ecc.) e che hanno necessità di accedere agevolmente alle informazioni giuridiche di propria competenza”³⁰².

Una delle peculiarità di questo progetto è individuabile nella volontà di realizzarlo coinvolgendo in questo processo le varie amministrazioni interessate, creando, di fatto una sorta di sistema federativo in cui ciascun soggetto mette in comune le proprie risorse giuridico documentali pur continuando a mantenerne il controllo e la gestione.³⁰³

Il progetto si è dato due obiettivi cardine:

1. Ideazione e realizzazione di soluzioni informatiche capaci di garantire comprensibilità e facilità nella ricerca;
2. Elaborazione di linguaggi informatici in grado di favorire la rappresentazione del testo normativo e l'agevole reperimento degli aspetti giuridicamente significativi.³⁰⁴

In questo contesto interviene la legge 388/2000 (legge finanziaria del 2001) il cui articolo 107 sotto la rubrica “*Informatizzazione della normativa vigente*” dispone l'istituzione di “un fondo destinato al finanziamento di iniziative volte a promuovere l'informatizzazione e la classificazione della normativa vigente al fine di facilitarne la ricerca e la consultazione gratuita da parte dei cittadini, nonché di fornire strumenti per l'attività di riordino normativo [...]”

Questo passaggio evidenzia come la questione dell'informatizzazione della normativa e della sua fruibilità venga acquisita fra le priorità da perseguire.

Occorre però sottolineare che le due iniziative, pur perseguendo un obiettivo riconducibile ad una medesima finalità, si caratterizzano per un diverso approccio quanto al modello adottato come riferimento: Se per Nir la forza propulsiva deriva esclusivamente dall'adesione volontaristica al progetto, non così, invece, nel secondo caso, per il quale viene delineato -dallo stesso art 107 - un modello di tipo piramidale in cui “il programma, le forme organizzative e le modalità di funzionamento del fondo sono determinati con decreto del Presidente del Consiglio dei ministri, previa intesa con il Presidente del Senato della Repubblica e con il Presidente della Camera dei deputati.”

Ed è appunto nel DPCM intitolato *Disposizioni per l'informatizzazione della normativa vigente, in attuazione dell'art. 107 della legge 23 dicembre 2000, n. 388*, del 24 gennaio 2003 che si individuano, all'art. 1 le attività da intraprendere:

³⁰² Cfr. Informatica e diritto, I / 2000, pag. 11.

³⁰³ Il progetto Norme in Rete si propone di elaborare un modello di cooperazione tra le Amministrazioni che consenta di ottenere il massimo della fruibilità dell'informazione pubblicata, costituendo nel contempo un volano in grado di sollecitare l'ampliamento dell'autonoma iniziativa di ciascuno Cfr. C. Lupo “Il progetto intersettoriale *Normeinrete*” cit. Ad oggi, le amministrazioni partecipanti al progetto risultano essere più di 50.

³⁰⁴ In ragione della sua spiccata connotazione tecnica, questo aspetto verrà approfondito al punto 3

- a) compilazione del testo delle leggi statali e degli altri atti normativi emanati dallo Stato, quale risultante dalle modifiche e abrogazioni espresse;
- b) messa a disposizione gratuita, con strumenti informatici e telematici, dei testi di cui alla lettera a), e delle relazioni afferenti al singolo atto normativo;
- c) classificazione della normativa vigente di cui alla lettera a) secondo parametri per favorire la ricerca per via informatica e telematica, nonché predisposizione di un idoneo apparato critico atto ad individuare profili di incompatibilità ed abrogazioni implicite fra disposizioni;
- d) studio ed applicazione di strumenti e procedure di ricerca raffinata della normativa vigente, nonché di sistemi avanzati di trattamento informatico, di marcatura e di classificazione degli atti normativi, anche ai fini dell'istruttoria dell'attività di riordino normativo;
- e) realizzazione di appositi portali e siti Internet, corredati da idonei motori di ricerca, ai fini delle attività di cui alle lettere precedenti.

Come specificato dall'art. 2 secondo comma, tali attività "sono definite in coordinamento con le iniziative già avviate nel campo della informatizzazione della documentazione giuridica pubblica"³⁰⁵

Con l'articolo 4 viene istituito un Comitato guida che ha il compito di:

- a) determinare gli indirizzi generali per l'attuazione del programma;
- b) definire gli obiettivi e la cadenza temporale per la realizzazione del programma di cui all'art. 2;
- c) definire i requisiti di ammissione al programma dei progetti di cui all'art. 3;
- d) definire le modalità e i termini per la redazione e la presentazione di progetti di implementazione del programma;
- e) valutare la conformità agli obiettivi del programma dei progetti ammissibili a finanziamento da parte del fondo;
- f) verificare lo stato di attuazione del programma e riferirne ai Presidenti delle Camere e al Presidente del Consiglio dei Ministri con cadenza almeno annuale.

Queste le principali fonti concernenti il tema dell'informatizzazione della normativa che permettono di avere un quadro degli orientamenti e delle azioni intraprese.

Nel passaggio alla realizzazione concreta di questi orientamenti e di queste azioni ci si trova ad affrontare un insieme di interrogativi e di problematiche di natura sia giuridica sia tecnica alle quali non sempre è facile dare risposta.³⁰⁶

³⁰⁵ Il programma di cui al art. 107 è cioè necessariamente portato, da un lato ad essere posto in relazione con il bagaglio di esperienze acquisite dal Ced della Corte di Cassazione e, d'altro canto, a non poter prescindere dalle tecnologie definite nell'ambito del progetto Nir. di cui rappresenta solo una delle possibili applicazioni.

³⁰⁶ Il reperimento delle informazioni di interesse normativo e giuridico presenta notevoli difficoltà, principalmente a causa della complessità propria della materia che, disciplinando i molteplici aspetti della vita sociale, dà luogo ad una quantità smisurata di informazioni, espresse in linguaggio naturale e quindi non strutturate, di una complessità e variabilità che riflettono quelle della realtà a cui si riferiscono, sempre più articolata ed in continua evoluzione. Cfr. Bollettino AIPA

Esiste, innanzi tutto, un problema squisitamente tecnico ed è quello della corretta e completa rappresentazione del testo giuridico.³⁰⁷

Occorre anche affrontare la questione di come rendere le differenti dimensioni temporali della norma (vigenza, efficacia, validità).³⁰⁸

Inoltre, considerata la mole degli atti giuridici esistenti è indispensabile, ai fini del trattamento informatico, effettuare una scelta distinguendo fra atti normativi e atti aventi natura non normativa³⁰⁹

Vediamo, qui di seguito, seppur brevemente, di tratteggiare gli aspetti specifici del processo tecnico di informatizzazione dei testi giuridici e di individuare le possibilità che questo processo può offrire ai fini del riordino e della semplificazione del corpus giuridico.

3. Analisi del processo tecnico di informatizzazione degli atti normativi, la rappresentazione informatica del testo normativo: problemi e procedure.

L'informatizzazione include due aspetti: l'uno, di tipo squisitamente tecnico legato alla qualità del testo informatizzato e l'altro inerente la ricognizione dell'insieme del corpus normativo³¹⁰.

La creazione di un servizio (o banca dati) che permetta di accedere al dato giuridico presuppone che si tenga conto di vari aspetti:

- quale caratterizzazione dare alla documentazione giuridica
- le varie esigenze degli utenti potenziali

Per rappresentare attraverso sistemi informatici il dato normativo occorre definire una serie di regole e procedure e disegnare un'architettura di sistema in grado di facilitare qualsiasi tipo di ricerca.

Questo lavoro preliminare è stato effettuato dallo Studio di fattibilità, realizzato dall'Istituto per la documentazione giuridica del CNR nell'ambito del progetto "Accesso alle norme in rete".³¹¹

Lo studio, dopo aver messo a punto una serie di considerazioni concernenti le caratteristiche e le modalità di accesso alle informazioni

³⁰⁷ Per una completa disanima di queste problematiche vedi il numero monografico della Rivista Informatica e diritto, I, 2000

³⁰⁸ "Ogni norma ha non meno di cinque "dimensioni temporali": (a) la prima riguarda la sua esistenza giuridica o appartenenza all'ordinamento; (b) la seconda riguarda ciò che chiameremo la sua vigenza (in un senso che si dovrà precisare); (c) la terza riguarda la sua validità; (d) la quarta riguarda la sua applicabilità da parte degli organi giurisdizionali ed amministrativi; (e) la quinta, infine, riguarda ciò che chiameremo la sua efficacia (in un senso di questa parola). Cfr. R. Guastini, "Teoria e dogmatica delle fonti", Giuffrè, 2002, pag. 169 ss; Vedi anche G. U. Rescigno, "L'atto normativo, Zanichelli, 1998, pag. 186 ss.

³⁰⁹ Cfr. G.U. Rescigno, op. cit. pag. 10 ss. in cui l'autore effettua un'attenta ed approfondita analisi dell'argomento.

³¹⁰ La scelta effettuata nell'ambito del settore pubblico è quella di costruire la base informativa includendo i testi normativi (non solo primari) risultanti dalle abrogazioni e dalle modifiche esplicite, a partire dal 1860. Si tratta di un lavoro immane considerando che "la Raccolta ufficiale delle leggi e dei decreti, iniziata nel 1861, anno della formazione del regno d'Italia, a fine anno 2000 aveva una consistenza intorno ai 1200 volumi. Non so quante siano le leggi e gli atti avente forza di legge vigenti contenuti in questi volumi. Non esiste alcuna indagine al riguardo." Cfr. R. Pagano, op. cit. pag. 8 ss.; vedi inoltre M. Ainis, op. cit. pag. 19 ss.; V. Di Ciolo, op. cit. pag. 35 ss.

³¹¹ Vedi il già citato numero monografico della rivista Informatica e diritto; vedi, inoltre sito NIR

giuridiche, i vari tipi di ricerca possibili e l'insieme delle problematiche inerenti la navigazione ipertestuale, gli indici per soggetti, e le funzionalità da prevedere per il sito progettato, tenendo conto dell'evoluzione della rete internet, ha affrontato l'aspetto relativo allo studio e alla definizione delle strutture dei testi giuridici, avvalendosi, per questo, del (meta) linguaggio XML³¹².

Ciò ha permesso di definire degli “standard di formato che permettono sia di rappresentare i testi normativi, sia di identificarli univocamente.

L'uso di linguaggi di marcatura come XML e di *editor* automatici per la realizzazione di documenti marcati in questo linguaggio, permettono la produzione e l'immissione in rete di documenti dotati d'una struttura formale altamente e, soprattutto, uniformemente elaborata.

L'attività di marcatura permette, quindi, di rendere maggiormente fruibile per mezzo delle tecnologie informatiche, l'insieme delle leggi e degli atti normativi e di facilitarne il riordino e la riorganizzazione³¹³

³¹² XML è un sistema informatico di marcatura “I sistemi di marcatura (mark-up) sono in grado di spostare sul dato, in questo caso lo stesso testo, la rappresentazione della meta-informazione, consentendone il trattamento. Identificando delle porzioni di testo in relazione al significato o alla funzione svolta, questa meta-informazione può essere utilizzata dai programmi in maniera funzionale al particolare scopo applicativo. Ad esempio, all'interno di un testo di legge, identificare il riferimento ad un'altra legge è una meta-informazione che può essere usata in modo diverso a seconda del supporto di riproduzione: se deve essere stampata, verrà usata per evidenziare il riferimento in corsivo, se deve essere pubblicata sul Web, questa conoscenza potrà essere usata per inserire automaticamente le informazioni necessarie a creare un hyperlink che permetterà di visualizzare la legge riferita. È noto che il “padre” dei linguaggi di marcatura è lo Standard Generalized Mark-up Language, SGML, nato negli Stati Uniti alla fine degli anni '70, divenuto poi standard dell'International Standard Organization (ISO 8879:1986). Il ricorso a SGML è rimasto limitato alle grandi organizzazioni, prevalentemente militari ed industriali, a causa della sua grande complessità, e del conseguente significativo investimento di tempo e risorse necessario a renderne proficuo l'utilizzo. In realtà l'SGML, piuttosto che un linguaggio di marcatura, è una specifica per generare propri sistemi di marcatura consentendo di creare centralmente le specifiche (DTD : Document Type Definition) che definiscono la struttura di documenti della stessa tipologia. L'HTML (Hypertext mark-up Language), così ampiamente affermatosi con il World Wide Web, altro non è che una particolare DTD di SGML, e quindi potremmo dire una sua particolare “istanza” . Nato proprio per gestire facilmente la presentazione delle pagine WEB, il suo punto di forza è diventato oggi il suo limite, in quanto è certamente facile da usare, ma non consente di andare oltre alla semplice presentazione delle informazioni. Ne è derivata l'esigenza di elaborare un linguaggio di marcatura che si collochi a metà strada tra i due, che sia in grado cioè di consentire agli utenti la definizione dei propri *tag* specifici per la tipologia di documenti trattati, di definire cioè le proprie DTD, ma in maniera più snella e semplificata rispetto a quanto prescritto da SGML. Da questa esigenza è nata, da parte del WWW Consortium (W3C), la specifica XML (*eXtensible Markup Language*). Come SGML, XML non si preoccupa degli aspetti legati alla presentazione, ma lascia la definizione degli aspetti tipografici agli *Style Sheet*, che vengono associati a classi di documenti omogenei o anche a singoli, e definiscono, in relazione ai marcatori di contenuto utilizzati, come deve avvenire la presentazione. Cfr: C. Lupo, Il progetto intersettoriale Normeinrete cit.

³¹³ Non è facile avere dati precisi circa la consistenza numerica del materiale normativo da riordinare, soprattutto perché risulta arduo definire criteri univoci su cui basare il calcolo; occorre infatti distinguere il numero delle leggi promulgate e pubblicate, (certo) dal numero delle leggi vigenti (incerto) in ogni caso, volendo considerare da un lato le leggi formali promulgate e pubblicate nel periodo 1861-2001, si arriva alla cifra di 30.339 leggi a livello statale (in media 217 ogni anno) e 35.786 leggi regionali; altrettanto interessante è poi la stima della consistenza numerica delle leggi statali (ed atti equiparati) vigenti, che, al 6 gennaio 1996, risultavano essere 12.725. Cfr. R. Pagano, *Introduzione alla legistica*, Giuffrè, 2004, pag. 9 e ss.

Il gruppo di lavoro sugli standard nell'ambito del progetto "Norme in rete", dopo aver studiato la struttura dei testi normativi, ha messo a punto uno "standard di formato" o Documento Tipo (Document Type Definition = DTD) che rispecchia l'organizzazione strutturale del documento da rappresentare.

Questo standard, elaborato allo scopo di permettere la rappresentazione dei testi normativi, viene indicato con l'acronimo Xml Nir

Il testo normativo è una struttura composta da una serie di elementi.³¹⁴ L'operazione di marcatura, volendo realizzarne una "rappresentazione", deve, innanzitutto:

- identificarne ed esplicitarne la sintassi (raffigurazione della struttura del documento normativo);
- rendere individuabile con certezza tanto il documento normativo nella sua interezza, quanto qualsiasi porzione testuale che concorre alla sua formazione al fine di renderla reperibile per qualsiasi tipo di ricerca;
- aggiungere informazioni destinate ad arricchire la conoscenza del documento normativo (meta dati).

Non esiste quindi un solo livello di marcatura, ma più livelli, che si sovrappongono, e lo standard Xml Nir permette di riconoscerli e di realizzare la descrizione del testo normativo nel modo più completo possibile.

In effetti la sintassi Xml Nir consente di definire un documento tipo nel quale vengono specificate le regole di correttezza strutturale del testo.

Ciò è reso possibile dal fatto che gli atti normativi sono organizzati secondo una determinata architettura³¹⁵, che è opportuno identificare ed illustrare prima di procedere all'esame dei singoli componenti.

Visto come oggetto strutturato e generale, un testo normativo consta di:

1. Porzioni di testo collocate all'inizio dell'atto, e cioè:
 - intestazione, nella quale viene inclusa:
 - ◇ la denominazione giuridica dell'atto;
 - ◇ la data di promulgazione (o emanazione)
 - ◇ il numero d'ordine dell'atto (se previsto);
 - ◇ il titolo dell'atto;
2. Porzioni testuali che costituiscono l'essenza dell'atto:
 - Preambolo o premessa
 - Formula di promulgazione
 - Testo degli articoli
3. Porzioni di testo conclusive:

³¹⁴ Per l'elaborazione dello standard si sono assunti, come riferimento, vari documenti che forniscono indicazioni, regole e raccomandazioni per la redazione dei testi normativi. In particolare la Circolare del Presidente del Senato della Repubblica, del presidente della Camera dei deputati e della presidenza del Consiglio dei ministri del 24 febbraio 1986 (G.U. n. 123 del 29 maggio 1986, Supplemento ordinario n. 401; il manuale sulle "Regole e suggerimenti per la redazione dei testi normativi redatto nel 1991 da una commissione di esperti e funzionari delle Regioni, del Parlamento e della Presidenza del Consiglio dei Ministri su incarico della Conferenza dei Presidenti di Assemblea, dei Consigli regionali e delle Province autonome, nonché la circolare della Presidenza del Consiglio del 20/04/2001 n. 10888.

³¹⁵ Come già detto, solo recentemente sono state formalizzate regole di redazione dei testi normativi, i testi precedenti richiedono, al redattore, una maggior attenzione.

- Formula finale
- Conclusione, che comprende:
 - ◇ Luogo e data
 - ◇ Sottoscrizioni
- Eventuali allegati

Nir parte dall'analisi di questa architettura e viene chiamato elemento radice poiché identifica l'approccio sintattico al testo normativo che ha permesso l'elaborazione di "etichette di riconoscimento" entro le quali racchiudere le varie porzioni di testo.

L'elaborazione dell'insieme di questi elementi, organicamente strutturati, assume una caratteristica struttura ad albero e si sviluppa secondo una precisa sequenza che procede dal generale e tende progressivamente a scendere verso il particolare permettendo, in questo modo, di definire tutti gli aspetti del documento.

Tuttavia, questa architettura si concretizza e specifica in singoli documenti normativi assumendo configurazioni di volta in volta differenti, in relazione alla varietà di procedimenti da cui essi possono trarre origine. In effetti, i documenti normativi possono presentare una vasta gamma di variazioni (soprattutto nella porzione che costituisce l'essenza del documento normativo) e la loro combinazione può divergere dalla linearità strutturale auspicata.

Per questa ragione Nir ha elaborato due schemi strutturali di riferimento uno funzionale alla marcatura di atti normativi redatti nel rispetto della Circolare 20 aprile 2001 e l'altro, più flessibile, da utilizzare per documenti normativi che presentano variazioni strutturali rispetto ad essa e per testi normativi redatti in precedenza.³¹⁶

I due schemi di riferimento identificano, entrambi, tredici differenti strutture che costituiscono i "calchi" o "impronte" entro i quali "adagiare" altrettante tipologie di atti normativi.

Queste strutture corrispondono alla tipologia di fonti normative contemplata dall'ordinamento e sono:

- Legge ordinaria (Legge)
- Legge costituzionale (LeggeCostituzionale)
- Decreto legge (DecretoLegge)
- Decreto legislativo (DecretoLegislativo)
- Decreto ministeriale numerato (DecretoMinisteriale)
- Decreto ministeriale non numerato (DecretoMinisterialeNN)
- Regio decreto (RegioDecreto)
- Decreto del Presidente della Repubblica numerato (Dpr)
- Decreto del Presidente della Repubblica non numerato (DprNN)
- Decreto del Presidente del Consiglio dei Ministri numerato (Dpcm)
- Decreto del Presidente del Consiglio dei Ministri non numerato (DpcmNN)

³¹⁶ Esiste anche un terzo schema o "calco" semplificato.

- Legge Regionale (LeggeRegionale)
- Atto di Authority (AttoDiAuthority)

Inoltre, nell'intento di garantire l'apertura dello standard, si è prevista la presenza di un numero limitato di strutture generiche cui ricorrere quando si tratta di sottoporre a marcatura un atto normativo che sia caratterizzato da una conformazione imprevista o, comunque non riconducibile a produzione normativa nazionale.

- Documento articolato (DocArticolato)
- Documento semi-articolato (SemiArticolato)
- Documento NIR (DocumentoNIR)
- Comunicato

Come si è accennato in precedenza, la marcatura tende a realizzare una descrizione del testo normativo al fine di renderne agevole la fruizione.

La comprensione del contenuto di un atto normativo, non dipende però unicamente dalla sua scomposizione in singoli fattori strutturali elementari, ma anche dalla possibilità di cogliere le diverse qualificazioni giuridiche che, di volta in volta, caratterizzano le singole disposizioni che concorrono alla formazione del dato testuale, lo standard messo a punto da XML Nir permette di realizzare un altro e distinto genere di marcatura – di tipo interpretativo – in grado di approfondire la comprensione del testo

In sostanza, oltre alla costruzione del portale Nir, il secondo risultato (ancor più rilevante) del progetto NormeInRete, è costituito dalla definizione di standard di formato per la rappresentazione dei testi normativi e per la loro univoca identificazione. Essi sono stati emanati con due circolari AIPA, rispettivamente:

- XML (eXtensible Mark-up Language), *CIRCOLARE n. AIPA/CR/40 del 22 aprile 2002 – Formato per la rappresentazione elettronica dei provvedimenti normativi tramite il linguaggio di marcatura XML*
- URN (Uniform Resources Name), *CIRCOLARE n. AIPA/CR/35 del 6 novembre 2001 – Assegnazione dei nomi uniformi ai documenti giuridici (vedi allegati)*

“L'adozione di tali standard permette di:

- predisporre automaticamente le funzionalità di navigazione ipertestuale tra riferimenti normativi;
- offrire funzionalità di ricerca per estremi identificativi e per parti strutturate del testo, in maniera uniforme su una base documentale distribuita;
- utilizzare lo stesso testo per scopi diversi: associando le direttive di presentazione all'interno di un cosiddetto “foglio di stile”, lo stesso *file* fisico può essere utilizzato indifferentemente per la stampa sulla Gazzetta, o per essere pubblicato su un sito web o inserito in una banca dati di un CD-ROM;
- realizzare sistemi di editing specializzato che, sfruttando le informazioni aggiuntive rappresentate con la marcatura XML, offrano funzionalità specializzate per la creazione ed il consolidamento dei testi normativi.”³¹⁷

³¹⁷ Cfr. F. Roller, *Le iniziative del Ministero della Giustizia per l'accesso alle leggi*, Atti del Convegno “Tante leggi: Come orientarsi ?” Roma 28 aprile 2004 in I quaderni Cnipa, n. 8.

Per tali aspetti l'esperienza italiana è considerata in Europa molto avanzata ed è seguita con attenzione anche da paesi extraeuropei.

La realizzazione e l'applicazione di questo linguaggio costituisce un elemento qualificante di notevole rilievo per le potenzialità offerte rispetto alle banche dati oggi esistenti che, per la rappresentazione testuale dei testi normativi fanno affidamento essenzialmente sul linguaggio HTML

I benefici di questo progetto sono di varia natura: ai cittadini NormeinRete offre un rapido accesso all'informazione giuridica; alle Amministrazioni Pubbliche offre un sistema di semplificazione ed interoperabilità; infine, ai professionisti fornisce vari strumenti di lavoro. NormeinRete è attivo dal 2000, oggi conta oltre 280.000 provvedimenti normativi "indicizzati", oltre 50 Amministrazioni partecipanti, più di 100.000 sessioni di ricerca al mese.³¹⁸

Altri progetti, derivanti dall'articolo 107 della legge 388/2000, come l'informatizzazione di tutta la normativa a partire dal 1861 "unitamente allo scopo di rendere effettivo per i cittadini l'esercizio del diritto di accesso alla norma vigente persegue esplicitamente un incremento di efficienza nell'azione di riordino, proponendosi di facilitare l'aggiornamento dei testi dei provvedimenti normativi, per loro natura in continua evoluzione"³¹⁹

4. L'informatizzazione come occasione per il riordino e la semplificazione del *corpus* normativo

Il processo di informatizzazione può certamente portare ad un più corretto rapporto fra le istituzioni ed i cittadini, ma per raggiungere un buon livello di efficacia e permettere che questi possano accedere non solo alle leggi ma anche all'iter di formazione delle norme (ad esempio progetti di legge, ecc..) è necessario che anche il legislatore sia ben consapevole del proprio ruolo e che la scrittura delle leggi diventi più semplice e più comprensibile, sia per quanto riguarda la struttura del testo che per il linguaggio usato.³²⁰

L'attenzione al modo in cui vengono redatte le leggi è piuttosto recente. Nel corso del tempo, su questo aspetto si sono pronunciati filosofi e uomini politici ma la loro attenzione si soffermava soprattutto sul rapporto fra le leggi e le società in cui vengono applicate³²¹, la preoccupazione era, quindi, di scrivere delle buone leggi più che quella di redigerle correttamente.

³¹⁸ Cfr. www.nir.it

³¹⁹ Cfr. C. Lupo, *L'utilizzo dell'ICT per il supporto alla gestione del ciclo di vita delle leggi: iniziative in tema di accesso e riordino delle norme* Atti del Convegno "Tante leggi: Come orientarsi ?" Roma 28 aprile 2004 in I quaderni Cnipa, n. 8.

³²⁰ "I problemi sono vari; uno di questi è come scrivere le norme affinché siano comprensibili e come scriverle in modo che il calcolatore le possa capire, infatti è necessario che la norma sia scritta e strutturata in un certo modo e che il calcolatore la possa capire, essendo questo molto veloce ma anche molto stupido" Cfr. P. L. Ridolfi, *Introduzione ai lavori* Atti del Convegno "Tante leggi: Come orientarsi ?" Roma 28 aprile 2004 in I quaderni Cnipa, n. 8.

³²¹ Vedi, ad esempio, quanto affermato da Montesquieu, il quale riteneva che le leggi devono aderire al popolo per cui sono scritte, devono tener conto della situazione del paese, clima, caratteristiche del

L'accresciuta complessità della società in cui viviamo, la molteplicità delle fonti normative (nazionali e comunitarie), gli effetti della globalizzazione, la rapidità delle trasformazioni economiche, delle innovazioni tecniche e scientifiche e la conseguente difficoltà a governare questi fenomeni ha visto nascere e svilupparsi una nuova attenzione e riflessione “sui modi di produzione delle norme e sulla loro qualità in termini di chiarezza, coerenza ed efficacia.. Si prende cioè consapevolezza che il miglioramento della qualità della legislazione non è solo un problema di carattere meramente tecnico-giuridico, ma che per le sue implicazioni sul piano istituzionale, sociale ed economico è anche un rilevante obiettivo politico, tanto da figurare, per la prima volta, perfino in un trattato internazionale (Dichiarazione n. 39 sulla qualità redazionale della legislazione comunitaria, allegata al Trattato di Amsterdam del 2 ottobre 1997) e nelle raccomandazioni di organizzazioni internazionali come l'OCSE, preoccupata delle incidenze economiche negative di una normazione mal formulata (Raccomandazione adottata dal Consiglio dell'OCSE nel 1995 sul miglioramento della qualità della normazione pubblica”³²².

La scarsa chiarezza dei testi normativi è, di fatto, un fattore di inquinamento dell'ordinamento che può manifestarsi in forme diverse³²³, e che può derivare da cause diverse, essa può essere originata da imprecisioni nella redazione del testo, o da ambiguità legate alla scelta dei termini o della formulazione, ma può anche derivare dall'esigenza del legislatore di preservare equilibri politici. Esiste, inoltre, anche un inquinamento quantitativo a causa del sovrapporsi di leggi e competenze che rendono difficile individuare la norma di riferimento.³²⁴

Molto è stato scritto questi argomenti e molto ancora si potrebbe dire ma è importante “sottolineare che una disposizione legislativa inestricabilmente oscura, tale cioè da non consentire al destinatario di comprenderne univocamente il significato (nonostante gli sforzi effettuati dal medesimo tramite la diligente consultazione di dottrina e giurisprudenza), è censurabile non solo sotto il profilo della tecnica legislativa, ma talvolta anche sotto quello – assai più importante e decisivo – della legittimità costituzionale della disposizione “oscura”³²⁵

In che modo, nella situazione fin qui descritta, il processo di informatizzazione può diventare un'occasione determinante per il riordino e la semplificazione del corpus normativo?

Secondo R. Pagano, “Vi è una stretta relazione tra tecnica legislativa e ottimizzazione dei sistemi di informatica giuridica, poiché l'adozione di una data tecnica legislativa in luogo di un'altra può influire in modo positivo o negativo sulla validità ed efficacia di risposta di una banca dati giuridici. A

territorio, tipo di vita dei suoi abitanti, tener conto del grado di libertà che la costituzione prevede, della religione ,ecc...”scritte per il popolo “

³²² Cfr. R.Pagano, “Introduzione alla legistica”, Giuffrè, 2004, pag. 6-7

³²³ Cfr. R.Pagano, op.cit, pag. 15-18

³²⁴ Vedi in proposito le opere dei già citati R.Pagano; M. Ainis e V. Di Ciolo

³²⁵ Cfr. V. Di Ciolo, op.cit., pag.27

sua volta una banca dati giuridici (norme e sentenze) risulta di grande aiuto al legislatore (e per esso al redattore di progetti di testi legislativi) facendogli risparmiare faticose ricerche ed evitare di ricadere in tecniche legislative errate o dannose, come, ad esempio, il frequente ricorso alla formula della abrogazione innominata.”³²⁶

L’esigenza di pervenire ad una semplificazione e ad un riordino del corpus normativo è sentita in modo sempre più pressante, prova ne sia l’emanazione di disposizione come quelle contenute nell’articolo 14, comma 14 della legge n. 246 del 2005³²⁷ che, avendo come obiettivo lo sfoltoimento dello stock normativo, delinea un percorso per cui a seguito di un procedimento complesso si giunga all’abrogazione di tutte le norme primarie emanate prima del 1970, tranne alcune eccezioni.

Questa norma, chiamata anche norma “ghigliottina”, pur partendo da un proposito condivisibile ha sollevato notevoli perplessità per ragioni di ordine costituzionale in merito alla ripartizione di competenze fra governo e parlamento, alla complessità del meccanismo prospettato e ai tempi attuazione. per cui molti giuristi sembrano ritenere che tale norma sia difficilmente applicabile.³²⁸

I progetti di informatizzazione che hanno preso vita in ambito pubblico (elaborazione dello standard Xml.Nir, progetto “107”- che sono stati brevemente illustrati nella prima parte di questo testo - e altre iniziative in via di realizzazione come i progetti: x-leges; c-leges; e r-leges³²⁹) possono, indubbiamente, fornire un apporto efficace e concreto al processo di semplificazione e di riordino del corpus normativo.

³²⁶ Cfr. R. Pagano. op. cit., pag. 83-84

³²⁷ “Entro ventiquattro mesi dalla scadenza del termine di cui al comma 12, il Governo è delegato ad adottare, con le modalità di cui all’articolo 20 della legge 15 marzo 1997, n. 59, e successive modificazioni, decreti legislativi che individuano le disposizioni legislative statali, pubblicate anteriormente al 1° gennaio 1970, anche se modificate con provvedimenti successivi, delle quali si ritiene indispensabile la permanenza in vigore, nel rispetto dell’articolo 1, comma 2, della *legge 5 giugno 2003, n. 131*, e secondo i seguenti principi e criteri direttivi: a) esclusione delle disposizioni oggetto di abrogazione tacita o implicita; b) esclusione delle disposizioni che abbiano esaurito o siano prive di effettivo contenuto normativo o siano comunque obsolete; c) identificazione delle disposizioni la cui abrogazione comporterebbe lesione dei diritti costituzionali dei cittadini; d) identificazione delle disposizioni indispensabili per la regolamentazione di ciascun settore, anche utilizzando a tal fine le procedure di analisi e verifica dell’impatto della regolazione; e) organizzazione delle disposizioni da mantenere in vigore per settori omogenei o per materie, secondo il contenuto precettivo di ciascuna di esse; f) garanzia della coerenza giuridica, logica e sistematica della normativa; g) identificazione delle disposizioni la cui abrogazione comporterebbe effetti anche indiretti sulla finanza pubblica.”

³²⁸ Cfr. L. Cuocolo “Aspetti problematici della legge di semplificazione per il 2005”, pubblicato su <http://www.associazionedeicostituzionalisti.it>,

³²⁹ X-leges affronta il tema dello scambio elettronico di documenti fra le istituzioni che prendono parte al processo di produzione legislativa. Lo scopo di c-leges è quello di mettere a confronto software per la classificazione automatica, al fine di determinare quale sia il programma che meglio risponde alle necessità istituzionali di classificazione. Il progetto r-leges è ancora allo stato iniziale ed è finalizzato la possibilità di offrire supporto alle attività di riordino normativo attraverso un’attività sperimentale da svolgersi in collaborazione con il mondo della ricerca. Vedi C.Lupo, “Beyond NormeinRete”, in I quaderni CNIPA n. 18, 3° Workshop on Legislative XML, nov. 2005

In particolare “gli interventi di informatizzazione previsti dal programma [107] non si limitano a favorire l’accesso ai documenti, ma sono indirizzati anche a fornire un efficace ausilio alla elaborazione dei testi vigenti e dei testi unici e pertanto rivolti al supporto di processi interni agli organismi istituzionali.

L’automazione del processo di produzione potrà, in una prospettiva di medio termine, avvenire a partire dalle prime fasi di drafting, all’interno delle Camere, del Dipartimento per gli affari giuridici e legislativi (DAGL) e degli Uffici legislativi delle Amministrazioni.

A questo scopo sono già in corso sperimentazioni per la generazione ed inserimento dei nuovi provvedimenti attraverso sistemi di editing specializzati. Tali editor, che potranno in futuro essere resi disponibili a tutti gli organismi che svolgono il ruolo di produttori o editori di norme, sono in grado di offrire:

- supporto al drafting, attraverso funzioni di editing mirate a favorire il rispetto delle regole di buona normazione come definite nelle circolari del Presidente del Consiglio dei Ministri.

- supporto alla costruzione dei testi vigenti, attraverso funzioni in grado di sfruttare la rappresentazione informazioni inserite nei testi, mediante la marcatura standard proposta, per segnalare le relazioni modificative tra le norme e supportare la creazione dei diversi testi vigenti nel tempo.

La sperimentazione per l’automazione del flusso documentale legato alla pubblicazione delle norme, deliberata dal Comitato Guida del programma ex 107 ed affidata al CNIPA, potrà creare le condizioni per un significativo salto di qualità..”³³⁰

5. Conclusioni

L’attenzione delle istituzioni alle tematiche che questo testo ha brevemente cercato di delineare, è certamente elevata, prova ne sia il recentissimo DPCM del 12 settembre 2006 intitolato: *Costituzione del Comitato interministeriale per l’indirizzo e la guida strategica delle politiche di semplificazione e di qualità della regolazione*. (G.U. n. 255 del 2-11-2006).

Come affermato da M. Pensato: “La divulgazione della legge, quale attività finalizzata a diffondere le norme in modo intelligibile, deve avvenire liberando i documenti legislativi da “incrostazioni e tecnicismi”.

Pur muovendo dal testo legislativo la divulgazione deve superarlo traducendone le forme giuridiche in espressioni intelligibili per il cittadino medio utilizzando metodi analoghi a quelli della pubblicità commerciale.

Naturalmente l’intervento di semplificazione normativa deve essere effettuato con rigore scientifico avendo cura di non tradire lo spirito e la ratio legis.

³³⁰ Cfr. C. Lupo, *L’utilizzo dell’ICT per il supporto alla gestione del ciclo di vita delle leggi: iniziative in tema di accesso e riordino delle norme* Atti del Convegno “Tante leggi: Come orientarsi ?” Roma 28 aprile 2004 in I quaderni Cnipa, n. 8.

L'attività di semplificazione normativa non può che riguardare atti definitivi (e, quindi, non disegni di legge). La divulgazione di testi normativi semplificati costituirà, quindi, un prezioso strumento per realizzare la conoscibilità effettiva delle regole giuridiche.

Questa linea di attività, si pone l'obiettivo, particolarmente ambizioso, di rendere effettivamente conoscibile il contenuto dei principali testi normativi non solo agli addetti ai lavori ma anche a coloro che non hanno competenze giuridico normative³³¹

Portare a compimento il processo di riordino e semplificazione del corpus normativo, oggi richiede, con sempre maggiore urgenza, di operare per "cercare di legare lo sviluppo delle tecniche a quello di una cultura della qualità della regolazione: senza di essa, infatti, gli sforzi sono destinati al fallimento o, peggio, all'eterogenesi dei fini, complicando, stratificando, ingarbugliando e infine scoraggiando, anziché semplificare. Rimane un ultimo punto da sottolineare, che forse è il più rilevante di quelli fin qui esaminati.....si tratta del finanziamento delle politiche di qualità della normazione .Si è già detto, infatti, che la qualità ha dei costi, e spesso molto elevati."³³²

7. Allegato 1.

Circolare del 6 novembre 2001, n. AIPA/CR/35.

(urn:nir:autorita.informatica.pubblica.amministrazione:circolare:2001-11-06;35)

"Assegnazione dei nomi uniformi ai documenti giuridici"

Gazzetta Ufficiale, Serie generale, n. 262 del 10 novembre 2001.

L'Autorità per l'informatica nella pubblica amministrazione ha avviato nel gennaio 1999 un progetto intersettoriale, denominato "Norme in rete", con l'obiettivo di favorire l'accesso alle norme da parte dei cittadini.

"Norme in rete" si sviluppa costruendo incrementalmente un portale dotato di funzionalità di ricerca che operano su documenti normativi accessibili nei siti web delle istituzioni e amministrazioni pubbliche che aderiscono al progetto. Le modalità di integrazione non risultano intrusive rispetto ai sistemi informatici delle istituzioni partecipanti. Attualmente aderiscono al progetto oltre 40 istituzioni.

Nel novembre 1999 la Camera dei deputati ha sollecitato il Governo a promuovere iniziative per consentire ai cittadini la consultazione gratuita dei testi normativi attraverso internet, facendo esplicito riferimento al progetto. L'aumento del numero di amministrazioni aderenti e di accessi al sistema hanno indotto l'Autorità, nel giugno del 2000, a proporre la costituzione di un Comitato tecnico interistituzionale, con compiti di indirizzo e di supervisione.

³³¹ Cfr. M. Pensato in Atti del Convegno "Tante leggi: Come orientarsi ?" Roma 28 aprile 2004 in I quaderni Cnipa, n. 8

³³² Cfr L. Cuocolo, cit.

Allo stadio attuale di sviluppo, sul portale www.normeinrete.it sono offerte funzionalità di ricerca uniformi della documentazione normativa disponibile sui diversi siti web istituzionali, mentre le funzionalità di navigazione ipertestuale sono quelle rese disponibili autonomamente da ciascun sito.

La possibilità di percorrere la rete dei riferimenti è determinante per la comprensione del dettato normativo e quindi per l'effettiva fruibilità delle norme da parte dei cittadini, delle imprese e degli altri operatori. D'altra parte, le attività redazionali necessarie richiedono un impegno di risorse considerevole e continuativo nel tempo.

I meccanismi di navigazione finora disponibili si basano sulla localizzazione fisica dei documenti. La definizione di convenzioni per identificarli in base ad elementi rappresentativi del contenuto consente di introdurre automatismi nella creazione dei collegamenti, favorendo così la creazione di un ipertesto delle risorse informative giuridiche distribuite sui siti web.

Si ritiene perciò utile avviare un processo di standardizzazione della rappresentazione informatica delle norme, definendo regole essenziali per la creazione di nomi uniformi dei provvedimenti normativi e giuridici italiani. Si rendono possibili, in questo modo, il riconoscimento di un riferimento normativo all'interno di un testo in linguaggio naturale e l'associazione del riferimento all'indirizzo fisico, realizzando funzionalità di navigazione ipertestuale.

Le regole introdotte sono state elaborate da un gruppo di lavoro istituito all'interno del progetto "Norme in rete"; esse adottano criteri di attribuzione di nomi (denominati URN, *Uniform Resource Name*) conformi a quelli definiti all'interno dell'IETF (*Internet Engineering Task Force*).

Le regole di composizione dei nomi e le modalità con cui effettuarne l'associazione ai provvedimenti sono accessibili sul sito www.aipa.it e sul sito www.normeinrete.it. Negli stessi siti sono indicate le istituzioni aderenti al progetto.

Sul sito www.normeinrete.it sono disponibili strumenti software per costruire il nome uniforme a partire dagli estremi identificativi di un provvedimento; essi possono essere utilizzati on-line per la generazione dell'URN, oppure scaricati sulla propria stazione di lavoro per inserire l'URN generato all'interno di documenti in formato HTML.

Nell'ambito delle attività di "Norme in rete" sono stati pure realizzati prototipi software, attualmente in fase di sperimentazione, per il riconoscimento dei riferimenti normativi all'interno di un testo, la creazione del nome uniforme ed il reperimento del relativo provvedimento, se pubblicato da una delle istituzioni aderenti al progetto. Terminata la sperimentazione, i servizi verranno resi disponibili sul sito www.normeinrete.it.

Si invitano le amministrazioni a valutare l'opportunità di aderire allo standard proposto e di adottare le misure tecniche necessarie per realizzare le funzionalità conseguenti.

Qualora aderissero al progetto "Norme in rete", potranno usufruire del supporto offerto al suo interno.

Roma, 6 novembre 2001

Il Presidente: ZULIANI

Per la consultazione delle regole di composizione dei nomi e le modalità con cui effettuarne l'associazione

ai provvedimenti si rimanda ai siti www.cnipa.gov.it e www.normeinrete.it

7. Allegato 2.

Circolare 22 aprile 2002 n. AIPA/CR/40

(urn:nir:autorita.informatica.pubblica. amministrazione:circolare:2002-04-22;40)

“Formato per la rappresentazione elettronica dei provvedimenti normativi tramite il linguaggio di marcatura XML”

Gazzetta Ufficiale n. 102 del 3 maggio 2002

A tutte le Amministrazioni pubbliche

1. PREMESSA

L'impulso istituzionale sui temi del riordino normativo e della qualità della regolazione persegue l'obiettivo di semplificazione del *corpus* normativo, attraverso azioni mirate a ridurre il numero delle norme e a favorirne la chiarezza. A tale scopo, la circolare del Presidente del Consiglio dei ministri del 20 aprile 2001, pubblicata nella *Gazzetta Ufficiale* del 27 aprile 2001, n. 97 (in seguito riferita come *circolare 2001*) ha riformato le regole alle quali le amministrazioni sono invitate ad attenersi nella redazione dei provvedimenti (cosiddetta attività di *drafting*). Tali regole sono state riformulate in maniera più analitica, ed integrate con riferimento alla redazione dei testi regolamentari, nella “Guida alla redazione dei testi normativi”, pubblicata nel supplemento ordinario alla *Gazzetta Ufficiale* del 3 maggio 2001, n. 101.

Per rendere effettiva la conoscibilità delle norme da parte dei cittadini è necessario che, accanto agli interventi di semplificazione, siano intraprese iniziative idonee a consentire l'accessibilità telematica alle norme, risolvendo i problemi di carattere giuridico e tecnologico che ne ostacolano l'attuazione.

La necessità di prevedere azioni finalizzate a consentire l'accessibilità telematica del *corpus* normativo trova una sua affermazione nel programma *e-Europe*, che colloca i dati giuridici tra i dati pubblici essenziali, classificati come prioritari, l'accessibilità dei quali è riconosciuta come diritto dei cittadini che gli Stati membri dell'Unione europea devono impegnarsi a garantire.

2. STANDARD PER LA RAPPRESENTAZIONE DEI PROVVEDIMENTI NORMATIVI

La diffusione di strumenti informatici per la produzione, il trattamento e la pubblicazione dei testi costituisce un fattore abilitante per perseguire gli

obiettivi citati, ma va accompagnata dalla definizione di regole e criteri volti ad accrescere l'efficacia e l'interoperabilità degli strumenti automatici di elaborazione e dei servizi connessi nel contesto specifico della produzione e pubblicazione di documenti a carattere normativo.

Il progetto intersettoriale dell'Aipa "Norme in rete" ha affrontato, nella sua prima fase, i problemi relativi all'uniformità delle funzioni di ricerca delle norme attraverso internet, indipendentemente dai formati di rappresentazione dei provvedimenti. È stato, quindi, realizzato un portale per l'accesso unificato ai documenti di interesse normativo pubblicati sui siti web istituzionali, ricorrendo alle tecnologie di indicizzazione e ricerca dei documenti in base alle parole presenti nel testo.

Parallelamente sono state avviate attività di standardizzazione finalizzate a favorire l'interoperabilità tra sistemi diversi e a consentire la realizzazione di funzionalità più specifiche. In particolare, sono state definite le regole per l'assegnazione di un nome identificativo univoco ai provvedimenti normativi, allo scopo di semplificare la realizzazione di funzionalità di navigazione ipertestuale tra basi documentali normative distinte e di migliorare l'efficacia delle funzioni di ricerca. Tale standard è stato divulgato attraverso la circolare 6 novembre 2001, n. AIPA/CR/35 "Assegnazione dei nomi uniformi ai documenti giuridici" (pubblicata nella *Gazzetta Ufficiale* del 10 novembre 2001, n. 262).

Un altro elemento determinante per la realizzazione di sistemi di elaborazione più efficaci è rappresentato dalla possibilità di identificare gli elementi costitutivi dei documenti appartenenti ad una stessa classe (come, ad esempio, gli elementi che costituiscono la struttura dei provvedimenti normativi quali: titolo, parti, articoli, commi e altro) e di associare ad essi altre informazioni che ne arricchiscano o qualifichino il contenuto. Tale integrazione del contenuto informativo di un testo può essere attuata con i linguaggi di marcatura (o *mark-up*) che forniscono le tecniche per associare ai documenti testuali, o a loro specifiche parti, informazioni aggiuntive.

La condivisione di un medesimo formalismo di marcatura dei testi normativi resi accessibili da organismi differenti, anche se dotati di sistemi informatici tecnologicamente eterogenei, consente di costruire un sistema di ricerca unitario, in grado di offrire funzionalità più efficaci ed un livello di precisione superiore a quello ottenibile con la semplice ricerca per parole. Inoltre, la marcatura dei provvedimenti normativi in base a regole definite consente di rappresentare informazioni relative anche a quelle specifiche parti del testo che contengono riferimenti ad altri provvedimenti e – soprattutto se attuata già a partire dalle fasi di *drafting* - rende possibile la realizzazione di sistemi informatici di supporto alle azioni di riordino normativo e di costruzione dei testi vigenti.

3. FORMALISMO DI RAPPRESENTAZIONE ADOTTATO

Il linguaggio di marcatura che offre la possibilità di definire strutture per classi omogenee di documenti e che si sta progressivamente affermando come standard nell'ambito della rete internet è l'*extensible markup language* (XML), già adottato dall'Aipa nella circolare 7 maggio 2001, n. AIPA/CR/28 (*Gazzetta Ufficiale* del 17 maggio 2001, n. 113) per rappresentare le informazioni da associare ai documenti scambiati attraverso i sistemi di protocollo informatico.

Il linguaggio XML consente di specificare vincoli di correttezza strutturale su una classe di documenti attraverso un formalismo di definizione di regole, denominato *document type definition* (DTD): ogni insieme di documenti che presenta caratteristiche uniformi può essere descritto con uno specifico DTD. Nell'ambito delle attività svolte dai gruppi di lavoro del progetto "Norme in rete", tale formalismo è stato adottato per rappresentare i principali tipi di atti normativi. La necessità di fornire regole di rappresentazione valide per diverse tipologie di provvedimenti e di affiancare ad esse una modalità di marcatura semplificata ha dato luogo alla definizione di tre DTD tra di loro compatibili in quanto adottano le medesime definizioni per gli elementi comuni. Essi, pur descrivendo all'incirca lo stesso insieme di provvedimenti, si differenziano per la rigidità dei vincoli imposti alla struttura del documento, come illustrato nel seguito:

- a) il *DTD base* descrive documenti che hanno una struttura molto semplice e regolare, non presentano eccezioni e rispettano le regole per la redazione dei documenti normativi espresse nella *circolare 2001*. L'attuazione della marcatura secondo le regole specificate in questo DTD risulta semplice e copre una casistica sufficientemente ampia. La sua maggiore semplicità facilita, inoltre, le fasi di sperimentazione;
- b) il *DTD completo* è in grado di descrivere documenti di struttura più complessa, ma anch'essi conformi alle prescrizioni della *circolare 2001*, rappresentando i vincoli nella numerazione e nella composizione delle parti della struttura previsti per ciascun tipo di atto. Dal momento che il DTD completo consente la gestione di una più estesa varietà di informazioni e strutture, esso risulta necessariamente più complesso;
- c) il *DTD flessibile* si adegua alle possibili strutture irregolari dei documenti normativi esistenti, permettendoci di descriverne le caratteristiche, anche se difformi dalle regole di tecnica legislativa previste per le norme più recenti, e permette di descrivere documenti che presentino eccezioni o particolarità.

4. I PROVVEDIMENTI DESCRITTI

provvedimenti normativi descritti dai tre DTD possono essere raggruppati, in funzione della loro struttura, in due categorie di documenti:

- a) il *documento articolato*, che prevede una struttura costituita da intestazione, formula iniziale (che può contenere un preambolo), articolato, formula finale, conclusione, eventuali annessi.

L'articolato è in genere strutturato secondo una rigida gerarchia nella quale ciascun componente ha una numerazione e una rubrica. I provvedimenti che riflettono la struttura del documento articolato sono: leggi, leggi costituzionali, decreti legge, decreti legislativi, decreti del Presidente della Repubblica, decreti del Presidente del Consiglio dei ministri, Regi Decreti, leggi regionali;

b) il *documento semi-articolato*, in cui sono previsti gli stessi elementi che compongono la struttura del documento articolato, ma senza vincoli sull'obbligatorietà della loro presenza e sull'ordine in cui compaiono. Oltre agli elementi previsti nella struttura, possono essere presenti elementi testuali arbitrari, non strutturati gerarchicamente. A questa categoria di documenti appartengono, ad esempio, gli atti di autorità, i decreti ministeriali non numerati, i decreti del Presidente della Repubblica non numerati e i decreti del Presidente del Consiglio dei ministri non numerati.

5. LA RAPPRESENTAZIONE DELLA STRUTTURA DEGLI ATTI

Gli elementi della struttura formale di un atto normativo, che vengono identificati attraverso specifiche modalità secondo le regole di marcatura proposte, sono:

- a) intestazione: ogni documento normativo possiede un'intestazione composta da un tipo di documento, una data, un numero d'ordine ed un titolo;
- b) formula iniziale: le formule di rito iniziali sono obbligate e ripetute tra tutti i documenti di uno stesso tipo e vengono opportunamente marcate. Essa contiene l'eventuale preambolo;
- c) articolato: l'articolato si compone di libro, parte, titolo, capo, sezione, paragrafo ed articolo secondo le regole di composizione relative a ciascun tipo di provvedimento.

Ogni elemento della gerarchia può avere una rubrica testuale ed un numero d'ordine;

- d) elementi interni all'articolo: un articolo è composto da commi, che contengono o un corpo di testo o elenchi composti di elementi lettera o di elementi numero, eventualmente tra loro nidificati.

Articoli e commi possono presentare la cosiddetta decorazione, che consente di specificare l'origine normativa dell'articolo stesso, aggiungendosi alla rubrica;

- e) formula finale: le formule di rito finali sono strutturate ed appositamente marcate;

f) conclusione: in essa viene identificata la parte in cui si specificano la data e il luogo in cui è stato firmato l'atto normativo. Il blocco di sottoscrizioni è composto dai sottoscrittenti e dal visto;

- g) annessi: un documento normativo può prevedere uno o più annessi, che possono essere semplici elementi testuali, grafici, tabelle o interi documenti strutturati. Le regole di marcatura prevedono sia la possibilità di porre il corpo dell'annesso all'interno del documento ospite, sia di rappresentarlo esternamente, in un documento autonomo.

Oltre agli elementi che rappresentano aspetti legati alla struttura degli atti normativi, i criteri di marcatura proposti permettono anche di identificare e di integrare informazioni che possono presentarsi ovunque all'interno del testo e che, nel contesto dei documenti normativi, rivestono un ruolo specifico. Tra questi, di notevole importanza sono i riferimenti normativi che contengono richiami ad altre norme. Tali riferimenti possono consistere in semplici citazioni o costituire lo strumento attraverso il quale hanno luogo interventi modificativi o abrogazioni. Una corretta e completa marcatura di queste parti consente la realizzazione di funzionalità di navigazione ipertestuale e di supporto alla costruzione dei testi vigenti.

6. META-INFORMAZIONI

Le meta-informazioni rappresentano informazioni che non fanno parte integrante del testo stesso, ma possono essere di interesse per gli utenti o utili ai fini delle elaborazioni automatiche.

I DTD di *Normeinrete* forniscono una sintassi per la rappresentazione delle metainformazioni, prevedendone cinque tipi:

- a) **descrittori**: sono alcune meta-informazioni fondamentali per descrivere il documento, come gli estremi della pubblicazione ufficiale, eventuali ripubblicazioni, il nome uniforme (secondo lo standard URN emanato con la citata circolare n. AIPA/CR/35), gli eventuali nomi alternativi usati nel linguaggio corrente (*alias*) con cui il documento è noto (ad esempio: “legge Merloni”), le vigenze, eventuali relazioni con altri documenti normativi e una lista di parole chiave per descrivere il documento;
- b) **lavori preparatori**: in questa sezione è possibile includere, a testo libero, informazioni e documenti connessi ai lavori preparatori relativi al provvedimento;
- c) **proprietario**: uno schema libero di meta-informazioni che ciascuna organizzazione che produce, gestisce o pubblica testi di provvedimenti normativi può liberamente definire per il raggiungimento di scopi applicativi specifici;
- d) **redazionale**: in questa sezione la redazione che si occupa di pubblicare un documento ha la possibilità di inserire informazioni libere sulla pubblicazione. Ad esempio, note di redazione o avvertenze;
- e) **disposizioni**: in questa sezione si possono inserire disposizioni caratterizzanti o analitiche per descrivere il contenuto normativo di un documento.

Le meta-informazioni rilevanti possono essere tante e di vario tipo e la definizione dei DTD fin qui messa a punto ne comprende solo alcune. Pertanto, è possibile che le evoluzioni future degli standard qui illustrati, a seguito di ulteriori approfondimenti o di nuovi contributi, diano luogo ad estensioni delle meta-informazioni.

7. LA RAPPRESENTAZIONE DELLA VIGENZA

I DTD di *Normeinrete* prevedono la rappresentazione di provvedimenti sia nel testo originale, sia in quello vigente ad una certa data ovvero in una forma redazionale in cui le modifiche intervenute fino alla specifica data stabilita sono riportate nel testo. È inoltre possibile rappresentare provvedimenti *multivigenti*, che riportano tutte le modifiche che si sono succedute nel tempo, con le corrispondenti date di validità. La rappresentazione del testo multivigente consente la realizzazione di applicazioni in grado di ricostruire dinamicamente il testo vigente in funzione di una data richiesta, non prestabilita.

8. DOCUMENTAZIONE DI SUPPORTO

Il formalismo di rappresentazione adottato per lo standard qui proposto si integra con le regole per l'associazione del nome uniforme a ciascun provvedimento definite nella citata circolare n. AIPA/CR/35. L'adozione di entrambi gli standard da parte delle pubbliche amministrazioni, consentendo l'interoperabilità tra le diverse basi documentali e la realizzazione di funzionalità di ricerca e di elaborazione più efficaci, contribuirà a favorire l'esercizio del diritto di accesso all'insieme dei dati pubblici costituito dai provvedimenti normativi.

L'allegato tecnico alla presente circolare introduce i fondamenti del linguaggio di marcatura adottato, costituisce una guida alla marcatura dei testi normativi secondo i DTD di *Normeinrete* e fornisce alcune indicazioni sugli strumenti software di supporto alle tecnologie adottate.

Sui siti www.aipa.it e www.normeinrete.it sono pubblicati i DTD con i necessari commenti esplicativi al loro interno, un glossario degli elementi e degli attributi adottati ed alcuni riferimenti tecnici.

Si invitano, pertanto, le amministrazioni a valutare l'opportunità di adottare lo standard proposto, eventualmente graduando nel tempo le conseguenti attività e definendo opportuni criteri di priorità.

Qualora le amministrazioni aderissero al progetto *Normeinrete*, le stesse potranno usufruire del supporto offerto al suo interno.

Roma, 22 aprile 2002

Il presidente f.f.: BATINI

Per la consultazione dell'allegato tecnico si rimanda ai siti www.cnipa.gov.it e www.normeinrete.it

7. Allegato 3.

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 12 settembre 2006

Costituzione del Comitato interministeriale per l'indirizzo e la guida strategica delle politiche di semplificazione e di qualità della regolazione. (GU n. 255 del 2-11-2006)

Art. 4.

Compiti e funzioni

1. Il Comitato predispone, entro il 31 marzo di ogni anno, un piano di azione per il perseguimento degli obiettivi del Governo in tema di semplificazione, di riassetto e di qualità della regolazione per l'anno successivo, individuando per ciascun obiettivo il soggetto o i soggetti responsabili per il suo conseguimento. Il piano, sentito il Consiglio di Stato, e' approvato dal Consiglio dei Ministri e trasmesso alle Camere.

2. Il Comitato coordina l'attività di realizzazione degli obiettivi del piano di azione da parte dei singoli responsabili, assicurando la coerenza delle varie iniziative e verifica periodicamente, con il supporto dell'unità per la semplificazione e del Dipartimento per la funzione pubblica della Presidenza del Consiglio dei Ministri, il loro stato di attuazione, che viene reso pubblico ogni sei mesi.

3. Al Comitato, sono sottoposte, per un esame preventivo all'approvazione da parte del Consiglio dei Ministri, le iniziative normative con prevalente finalità di semplificazione ed in particolare del disegno di legge di semplificazione. Nei lavori parlamentari relativi a detto disegno di legge il Governo e' rappresentato dal Sottosegretario alla Presidenza del Consiglio, designato dal Presidente del Consiglio, e dal Ministro per le riforme e le innovazioni nella pubblica amministrazione.

4. Il Comitato svolge, inoltre, funzioni di indirizzo, di coordinamento e, ove necessario, di impulso delle amministrazioni dello Stato nelle politiche della semplificazione, del riassetto e della qualità della regolazione. Nell'esercizio di tali compiti il Comitato provvede a:

a) richiedere un approfondimento dell'esame delle iniziative normative del Governo in caso di proposte che non appaiano necessarie o giustificate relativamente al rapporto tra costi e benefici o alla coerenza con gli obiettivi del piano di azione annuale di cui al comma 1;

b) individuare e sostenere iniziative non normative di semplificazione, anche tramite progetti di innovazione tecnologica o amministrativa, di comunicazione e di formazione;

c) monitorare, con le opportune procedure di verifica di impatto, l'efficacia delle misure di semplificazione introdotte e della loro effettiva applicazione, e prospettare, ove necessario, interventi correttivi;

d) convocare periodicamente il tavolo permanente per la semplificazione, di cui all'art. 5, individuare altre forme e modalità stabili di consultazione con le organizzazioni rappresentative degli interessi della società civile, e prevedere, ove possibile in via elettronica, forme di pubblicizzazione di tale attività, coordinando la consultazione in via telematica di cui all'art. 18 della legge 29 luglio 2003, n. 229, ed all'art. 55 del decreto legislativo 7 marzo 2005, n. 82. L'unità per la semplificazione assicura il supporto tecnico alle attività di consultazione.

5. Il Comitato assicura, infine, il costante raccordo con gli altri soggetti istituzionali e con gli altri livelli di governo in tema di semplificazione e di qualità della regolazione.

ASSOCIAZIONE D-LEX: DIRITTO & TECNOLOGIA

D-Lex è un'organizzazione no profit che si propone di promuovere e diffondere la cultura della Società dell'Informazione ed in particolare del diritto dell'informatica, dell'informatica giuridica e del diritto delle nuove tecnologie, attraverso la promozione e la diffusione di studi, iniziative e attività di ricerca, l'organizzazione di corsi di formazione, qualificazione e aggiornamento professionale, convegni, seminari, tavole rotonde, giornate di studio, *brainstorming* e incontri di approfondimento sulle medesime materie, nonché l'ideazione, la produzione, la creazione, la promozione e la gestione di attività editoriali, informative e di comunicazione in genere nelle medesime materie e in quelle ad esse correlate.

L'Associazione ha altresì lo scopo di fornire informazioni e assistenza nel settore del diritto dell'informatica e delle nuove tecnologie a chiunque abbia interesse in tali materie, su ogni tipologia di problematica relativa alla giuritecnica, nonché fornire agli iscritti agli albi professionali forensi la formazione professionale obbligatoria prevista dalle norme di legge e deontologiche.

L'associazione ha l'ambizione di costituire un punto di partenza sia per chiunque voglia avvicinarsi per la prima volta al diritto delle nuove tecnologie digitali, sia un punto di riferimento per chi, giurista, informatico o semplicemente curioso, è da sempre interessato all'unione tra il digitale e la scienza sociale per eccellenza.

L'obiettivo è quello di guardare al mondo dell'informatica giuridica con gli occhi del pragmatico e con un approccio il più concreto possibile. Così, pur mantenendo la giusta considerazione per i presupposti teorici e persino sociologici e filosofici della giuritecnica, l'attenzione è rivolta soprattutto al risvolto applicativo e pratico del connubio tra ICT e mondo del diritto, così come delle conseguenze giuridiche dell'impatto delle tecnologie elettroniche nella vita di tutti i giorni.

Per ulteriori informazioni consultare il sito www.d-lex.org

Lo staff D-Lex

BIBLIOGRAFIA

AA. VV., *Parola chiave: informazione. Appunti di diritto, economia e filosofia*, a cura di AGATA C. AMATO MANGIAMELI, Milano, Giuffrè, 2004.

AA. VV., *E-government. Profili teorici ed applicazioni pratiche del governo digitale*, a cura di FULVIO SARZANA DI SANT'IPPOLITO, Piacenza, La Tribuna, 2003.

AA. VV. *Trattato di diritto amministrativo*, a cura di SABINO CASSESE, 2^a ed., Milano, Giuffrè, 2003.

AA. VV., *Dalla giuritecnica all'informatica giuridica, studi dedicati a Vittorio Frosini*, a cura di DONATO A. LIMONE, Milano, Giuffrè, 1995.

AA. VV., *I problemi giuridici di Internet, diritto dell'Informatica* - a cura di E. TOSI, Milano, Giuffrè, 1999.

AA. VV. *Attualità forensi*, pubblicazione a cura della "Fondazione dell'Avvocatura Italiana" presso il Consiglio Nazionale Forense (annate 1998 – 2007).

AA. VV., *Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione* (2004 CNIPA).

AA.VV., *Linee Guida per la sicurezza ICT delle PP.AA.* (2006 CNIPA).

AA. VV., *Crimine virtuale, minaccia reale, ICT Security: politiche e strumenti di prevenzione*, Milano, Franco Angeli, 2004.

AA. VV., *Inside Attack – Manuale investigativo del computer crime aziendale*, Roma, Nuovo studio tecna edizioni, 2005.

AA. VV., Atti del Convegno "*Il patrimonio informativo della P.A. come servizio. I dati pubblici sono pubblici?*", Forum P.A., maggio 2000.

AA. VV., Atti del Convegno "*Tante leggi: come orientarsi?*" in Quaderno CNIPA n. 8, aprile 2004.

AA. VV., Atti del *III Workshop on legislative XML* in Quaderno CNIPA n. 18. novembre 2005.

AA. VV., *Elementi di informatica giuridica*, a cura di M. JORI Torino, Giappichelli, 2006.

AA. VV., *Trattamento dei dati e tutela della persona*, a cura di V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, Milano, Giuffrè, 1998.

AA.VV., *Il nuovo diritto*, a cura di Roberto Tomei Milano, Giuffrè, 2006.

AA.VV., *Diritto e società dell'informazione: riflessioni su informatica giuridica e diritto dell'informatica*, Milano, Nyberg, 2005.

AA.VV., *Le strategie competitive nel retail banking: segmentazione della clientela, modelli organizzativi e politiche commerciali*, a cura di Maurizio Baravelli, Anna Omarini Roma, Bancaria, 2005.

AA.VV., *Lineamenti di informatica giuridica*, a cura di Roberta Mannucci, Napoli Roma, ESI, 2002.

AINIS M., *La legge oscura*, Bari, Laterza, 2002.

ALPA G., “La normativa sui dati personali. Modelli di lettura e problemi esegetici”, in *Diritto dell'informazione e dell'informatica*, n. 4, 1997.

BARBIERO A., SPAGNOLO L., OSIMO D., *L'e-procurement nella Pubblica Amministrazione: guida pratica all'acquisto on-line di beni e servizi*, Rimini, Maggioli, 2001.

BELISARIO E., “Protocollo informatico: automazione di un registro o primo passo verso il procedimento amministrativo elettronico?”, al sito: www.telejus.it/articoli/articolo16-3.html.

BERGHELLA F., *Guida alle misure di sicurezza per la privacy*, Roma, Bancaria Editrice, 2006.

BIFFI A., FILOTTO U., *Soluzione banca virtuale*, Milano, SDA Bocconi – SMAU, 1997

BOMBARDELLI M., “Diritto di accesso e tutela della privacy”, in *Giornale di diritto amministrativo*, n. 5, 2000.

BOMBARDELLI M., “Nuovi orientamenti giurisprudenziali sul rapporto fra diritto di accesso e riservatezza”, in *Giornale di diritto amministrativo*, n. 6, 1999.

BORRUSO R., MATTIOLI L., *Computer e documentazione giuridica - teoria e pratica della ricerca*, Milano, Giuffrè, 1999.

BORRUSO R., *La legge, il giudice, il computer. Un tema fondamentale dell'informatica giuridica*, Milano, Giuffrè, 1997.

BRACCHI G., FRANCALANCI C., GIORGINO M., *Internet Banking*, Milano, Egea, 2000.

BRAVO F., “Le convenzioni con gli enti certificatori di firma digitale”, in *I Contratti*, n. 5, 2003.

BRUNETTI D., *Il codice della amministrazione digitale e la gestione elettronica dei documenti*, in *Comuni d'Italia*, n. 10, 2005.

BRUNETTI D., *La gestione informatica del protocollo, dei documenti e degli archivi*, Rimini, Maggioli, 2005.

BUONAMASSA R., *Le fonti del diritto nel mondo dell'informatica*, Bari, Cacucci, 2006.

BUTTARELLI G., *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997.

BUSCEMA V., "Discrezionalità amministrativa e reti neurali artificiali", in *Il foro italiano*, n. 2-3, pt. 1, 1993.

CAMMARATA M. – MACCARONE E., *La firma digitale sicura - il documento Informatico nell'ordinamento italiano*, Milano, Giuffrè, 2003.

CAMON F., *Le intercettazioni nel processo penale*, Milano, Giuffrè, 1996.

CAMPOMORI F., *Dematerializzazione dei documenti contabili e fiscali*, Milano, il Sole 24 Ore, 2006.

CAPRIOLI M., *Intercettazioni e registrazioni di colloqui tra persone presenti nel passaggio dal vecchio al nuovo c.p.p.*, in *Riv. it. dir. e proc. pen.*, 1991.

CARIDI G., PELLECCIA S., *Automazione della ricerca e sistemi esperti*, Milano, F. Angeli, 1986.

CARIDI G., *Informatica giuridica e procedimenti amministrativi*, Milano, 1983.

CARINGELLA F., *Corso di diritto amministrativo*, 3^a ed., Milano, Giuffrè, 2005.

CARINGELLA F., DELPINO L., DEL GIUDICE F., *Diritto Amministrativo*, Napoli, Novene, 2004.

CARNELUTTI F., "Documento (teoria moderna)" in *Novissimo digesto italiano*, VI, Torino, 1975.

CASSETTA E., *Manuale di diritto amministrativo*, 7^a ed., Milano, Giuffrè, 2005.

CASSANO G., *Diritto dell'Internet: il sistema di tutele della persona*, Milano, Giuffrè, 2005.

CLARIZIA R., "Il documento informatico sottoscritto: alcune note a margine del codice dell'amministrazione digitale", in *Diritto dell'Internet*, n. 3, 2005.

CONSO C. - GREVI V., *Compendio di procedura penale*, Padova, Cedam, 2005.

CONSO G., “intercettazioni telefoniche: troppe e troppo facilmente divulgabili”, in *Dir. pen. e processo*, 2007.

CORDERO F., *Procedura penale*, Milano, Giuffrè, 2006.

DAINESI E., *Netbanking, Banche e utenti dialogano su Internet*, Milano, Apogeo, 2000.

DE PETRIS D., *Valutazione amministrativa e discrezionalità tecnica*, Padova, Cedam, 1995.

DI CIOLO V., *La progettazione legislativa in Italia*, Milano, Giuffrè, 2002.

DRAETTA U. *Internet e commercio elettronico. Nel diritto internazionale dei privati*. Milano, Giuffrè, 2005.

DUNI G., “Il procedimento amministrativo tra l. 7 agosto 1990 n. 241 ed introduzione dell’amministrazione telematica”, in *Il foro amministrativo C.d.S.*, n. 1, 1995.

DUNI G., “Teleamministrazione”, in *Enciclopedia giuridica*, XXX, Roma, 1993.

DUNI G., *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato in forma elettronica*, in www.privacy.it/duni19780601.html.

EVANGELISTI U., *Documentazione amministrativa. Legalizzazione e autenticazione di Firme, rilascio di copie di atti*, Firenze, Nocchioli, 1971.

FAMELI E., “Intelligenza artificiale e sistemi esperti nel diritto. Note in tema di apprendimento e di ragionamento per analogia”, in *Informatica e diritto*, n. 10, 1984.

FANTIGROSSI U., *Automazione e pubblica amministrazione*, Bologna, 1993.

FINDACA G. – MUSCO E., *Diritto Penale parte generale*, Giappichelli, 2007.

FINDACA G. – MUSCO E., *Diritto Penale parte speciale*, Giappichelli, 2008.

FROSINI V., “L'informatica e la pubblica amministrazione”, in *Rivista trimestrale di diritto pubblico*, n. 2, 1983.

FUGINI M., MAIO F., PLEBANI P., *Sicurezza dei sistemi informativi*, Milano, Apogeo, 2001.

GAMBINO A., “Firma digitale”, in *Enciclopedia giuridica*, agg. VIII, Roma, 2002.

GASPARRI P., “Eccesso di potere (diritto amministrativo)”, in *Enciclopedia del diritto*, XIV, Milano, 1965.

- GIACCHETTI S., “Certificazione”, in *Enciclopedia giuridica*, X, Roma, 1993.
- GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, Cedam, 2001.
- GIANNINI M. S., *Istituzioni di diritto amministrativo*, 2^a ed., Milano, Giuffrè, 2000.
- GIANNINI M. S., “Atto amministrativo”, in *Enciclopedia del diritto*, IV, Milano, 1959.
- GIURDANELLA C., GUARNACCIA E., *Elementi di diritto amministrativo elettronico*, Macerata, Halley Editrice, 2005.
- GIURDANELLA C., GUARNACCIA E., “Amministrazione digitale: leggiamo il Codice”, al sito: www.interlex.it/pa/giurguar1.htm.
- GUASTINI R., *Teoria e dogmatica delle fonti*, Milano, Giuffrè, 1998.
- IASELLI M., *Open Source e PA, ci sarà un futuro?*, <http://www.studiocelentano.it>, 2006.
- LARATRO A., *La comunicazione esterna del web banking*, Università di Roma Tre, Roma, 2003.
- LONGONI M., *Istruzioni legali per l'uso di internet e-commerce*. Roma, Ed. Italia Oggi, 2000.
- LOSANO M. G., “Informatica giuridica”, in *Enciclopedia delle scienze sociali*, IV, Roma, 1994.
- LOSANO M. G., *L'informatica e l'analisi delle procedure giuridiche*, Milano, Unicopli, 1989.
- LUCATUORTO P., *Intelligenza artificiale e diritto: le applicazioni giuridiche dei sistemi esperti*, in *Cyberspazio e diritto*, n.2, 2006.
- MANTOVANI F. *Diritto penale*, Padova, Cedam, 2003.
- MARIANI B., TISCORNIA D., *Sistemi Esperti giuridici, L'intelligenza artificiale applicata al diritto*, Milano, F. Angeli, 1989.
- MARTINO A. A., *Sistemi Esperti nel diritto. Selezione di contributi al III Convegno internazionale di Logica, informatica e diritto*, Padova, Cedam, 1989.
- MASUCCI A., “Atto amministrativo informatico”, in *Enciclopedia del diritto*, I, Milano, 1997.
- MASUCCI A., *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Napoli, Jovene, 1993.

- MERCATALI P., *Informatica applicata alla pubblica amministrazione*, Napoli, Simone, 2003.
- MERCATALI P., SODA G., TISCORNIA D., *Progetti di intelligenza artificiale per la pubblica amministrazione*, Milano, F. Angeli, 1996.
- MIELI G. – BORGHI P., *Guida alla privacy nel rapporto di lavoro*; Roma, Bancaria Editrice, 2005.
- MINERVA M., “L’attività amministrativa in forma elettronica”, in *Il foro amministrativo*, n. 4, 1997.
- MITNICK, K. – SIMON W., *L’arte dell’inganno I consigli dell’hacker più famoso del mondo*; Roma, Feltrinelli, 2005.
- MITNICK, K., *L’arte dell’intrusione*; Roma, Feltrinelli, 2006.
- MODUGNO F., MANETTI M., “Eccesso di potere. Eccesso di potere amministrativo”, in *Enciclopedia giuridica*, X, Roma, 1989.
- MUSACCHIO V., “Brevi note sulla funzionalità delle intercettazioni nel nuovo c.p.p.”, in *Il Nuovo diritto*, n.2, 1995.
- NATALINI A., “Sistemi informativi e procedimenti amministrativi”, in *Rivista Trimestrale di Diritto Pubblico*, n. 2, 1999.
- NATOLI M., “Ambiti di operatività della discrezionalità amministrativa e di quella tecnica alla luce dell’informatizzazione dell’attività amministrativa”, in *Rassegna dell’avvocatura dello stato*, n.2, 2004.
- OROFINO A. G., “L’automazione amministrativa: imputazione e responsabilità”, in *Giornale di diritto amministrativo*, n. 12, 2005.
- OROFINO A. G., “La patologia dell’atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela”, in *Il foro amministrativo*, n. 9, 2002.
- PANZIERI S., SCARANO I., SETOLA , *Vulnerabilità informatica dei sistemi SCADA connessi alle reti pubbliche*; e-book pubblicato presso il sito: <http://panzieri.dia.uniroma3.it/Articoli/VGR2004.pdf>.
- PAGANO R., *Introduzione alla legistica*, Milano, Giuffrè, 2004.
- PARTITI R., ZANINI U., “La tenuta e la conservazione delle scritture contabili in formato digitale”, in *Il Fisco* n. 8, 2006.
- PASCUZZI G., *Il diritto dell’era digitale: tecnologie informatiche e regole privatistiche*, Bologna, Il mulino, 2002.

PECENIK M., *Web Banking - Indagine alla scoperta delle banche italiane in rete*, Milano, Simone, 2000.

PECORELLA C., *Diritto penale dell'informatica*, Padova, Cedam, 2006.

PEDACI V., "Note intorno alle nozioni di potere discrezionale ed attività vincolata della Pubblica Amministrazione", in *Nuova rassegna di legislazione, dottrina e giurisprudenza*, n. 21-22, 1996.

PERÈZ LUNO A. E., *Saggi di Informatica Giuridica*, Milano, Giuffrè, 1998.

PFLEEGER C., PFLEEGER S., *Sicurezza in informatica*, Pearson Education Italia, 2004.

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, UTET, 1999.

PIRAINO S., *La Funzione Amministrativa fra discrezionalità e arbitrio*, Milano, Giuffrè, 1990.

PIRAS A., "Discrezionalità amministrativa", in *Enciclopedia del diritto*, XIII, Milano, 1964.

PUDDU S., *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, Napoli, Jovene, 2006.

PUPILELLA R., "Dall'atto amministrativo all'e-government: un nuovo modello di amministrazione?", sul sito: www.diritto.it/articoli/amministrativo/pupilella1.html.

RAMAJOLI S., *La prova nel processo penale*, Padova, Cedam, 1995.

RESCIGNO G. U., *L'atto normativo*, Bologna, Zanichelli, 2002.

RIDOLFI P., *Firma elettronica: tecniche, norme, applicazioni*, Milano, F. Angeli, 2003.

ROSCINI VITALI F., "Archivi ottici, limitato il ricorso ai notai", in *il Sole 24 Ore*, 7 gennaio 2006;

ROSSELLO C., *Commercio elettronico. La governance di Internet tra diritto statale, autodisciplina, soft law e lex mercatoria*. Milano, Giuffrè, 2006.

SANDULLI A. M., "Documento (diritto amministrativo)" in *Enciclopedia del diritto*, XIII, Milano, 1964.

SANDULLI A., *La proporzionalità dell'azione amministrativa*, Padova, Cedam, 1998.

SANDULLI A., "La riduzione dei limiti all'accesso ai documenti amministrativi", in *Giornale di diritto amministrativo*, n. 11, 1997.

SCALA A., “L’automazione nella redazione degli atti amministrativi”, in *Nuova rassegna*, n. 17, 1995.

SELLERI B., “Gli atti amministrativi in forma elettronica”, in *Diritto e società*, n. 1, 1982.

SISSA G. *Open Source e PA*, in *Mondo Digitale* n. 3, 2003.

SPANGHER G., *La disciplina italiana delle intercettazioni di conversazioni o di comunicazioni*, relazione al convegno di Urbino del 10-12 marzo 1994.

STALLINGS W., *Sicurezza delle reti - applicazioni e standard*, Addison-Wesley Italia, 2004.

STILO L., *Il documento elettronico nella società dell’informazione*, in *Il Nuovo diritto*, n. 9, 2004.

TADDEI ELMI G., “Società artificiali e diritto”, al sito: www.altalex.com/index.php?idstr=30&idnot=7459.

TERRACCIANO G., “L’applicazione in campo giuridico delle reti neurali artificiali. Il programma GiuriNet”, in *I tribunali amministrativi regionali*, n. 12, pt. 2, 1998.

TONINI P., *Manuale di procedura penale*, Milano, Giuffrè, 2007;

USAI A., “Le prospettive di automazione delle decisioni Amministrative in un sistema di teleamministrazione”, in *Diritto dell’informazione e dell’informatica*, n. 1, 1993.

ZILLI S., “ODF di Open Office approvato ISO 26300”, <http://www.azpoint.net>, 2007.

DOCUMENTI PUBBLICI

“Indagine conoscitiva sul software a codice sorgente aperto”, <http://www.innovazione.gov.it>, 2003.

“Rapporto conclusivo del Gruppo di lavoro - Codice sorgente aperto”, <http://www.cnipa.gov.it>, 2004.

“Questione di libertà o sviluppo”, <http://www.forumpa.it>, 2006.

“Open source, continua il dibattito”, <http://www.forumpa.it>, 2006.

“*Stanca emana la Direttiva per l’Open Source nella PA*”, Comunicato stampa a cura dell’Ufficio stampa del Ministero per l’Innovazione e le Tecnologie, 2003.

“*L’Osservatorio Open source presso il CNIPA*”, <http://www.ossipa.cnipa.it>, 2006.

“*Software open e libero: gli enti locali guidano l’innovazione, dalla Provincia di Pisa l’Assessore Buongiovanni*”, <http://www.interlex.it>, 2003.

“*Linee Guida del Governo per lo sviluppo della Società dell’Informazione*”, Roma, 2002.

“*Fr: Court of Cassation turns to Open Source*”, copyright European Communities <http://ec.europa.eu>, 2006.

“*In Baviera vince l’OS*”, <http://www.punto-informatico.it>, 2003.

“*Monaco partorisce il suo Linux*”, <http://www.punto-informatico.it>, 2006.

“*Open source consacrato dall’ISO*”, <http://www.punto-informatico.it>, 2006.

“*Open Office: retroscena storico*”, <http://it.openoffice.org>, 2006.

“*DK: Danish reports forecast major savings from a danish public sector switch to ODF*”, OS News, <http://ec.europa.eu>, 2007.

“*Il Belgio adotta il formato Open Document*”, <http://www.punto-informatico.it>, 2006.

“*Parigi: l’Europa marci verso Open Document*”, <http://www.punto-informatico.it>, 2006.



a cura dell'associazione D-Lex