# UNIVERSITA' DEGLI STUDI DI MACERATA

## Facoltà di Lettere e Filosofia
## Facoltà di Economia
## Facoltà di Beni Culturali

**Master in**

**"Formazione, gestione e conservazione di archivi digitali**

**in ambito pubblico e privato"**

**III[a] edizione  Anno Accademico 2009-10**

# C.A.D. E PRIVACY:
# NUOVE RESPONSABILITA' IN NUOVI SCENARI

**Corsista :  FEDERICA MORICHETTI**

**Relatore:  PROF.SSA BARBARA MALAISI**

## INDICE

**INTRODUZIONE** **pag. 3**

**CAPITOLO I** **pag. 4**
***Il Concetto di Responsabilità nel panorama digitale.***

**CAPITOLO II** **pag. 7**
***Sicurezza Dati e Responsabilità.***

**CAPITOLO III** **pag. 10**
***Firma Digitale e Responsabilità.***

**CAPITOLO IV** **pag. 13**
***Posta Elettronica Certificata e Responsabilità.***

**CAPITOLO V** **pag. 15**
***La Responsabilità della Pubblica Amministrazione nella gestione del dato nel sito istituzionale.***

**CAPITOLO VI** **pag. 20**
***Conclusioni.***

**BIBLIOGRAFIA** **pag. 24**

# C.A.D. E PRIVACY:
# NUOVE RESPONSABILITA' IN NUOVI SCENARI

## *INTRODUZIONE*

L'obiettivo principale di questa tesi vuole essere quello di evidenziare l'impatto che le nuove tecnologie hanno sulle nostre azioni quotidiane sia come cittadini che nei contesti lavorativi, nelle relazioni con le istituzioni e con ogni altro soggetto di diritto. L'analisi viene condotta seguendo una prospettiva meramente giuridica che intende far luce sul concetto di "*responsabilità"*derivante dalle "nostre azioni tecnologiche". Infatti, molto spesso, non ci si sofferma a pensare che il mondo IT (*Information Technology*) in cui siamo proiettati e sempre di più catapultati, è una realtà dove l'aggettivo *nuova* significa diversa perché differenti sono gli elementi che la caratterizzano.

Tutto questo comporta il dovere di imparare nuovi linguaggi, di utilizzare nuove forme di comunicazione, di modificare alcune nostre abitudini e di assumere, nel contempo, comportamenti differenti da quelli tradizionali (non a caso oggi parliamo di un *Social Network* quale *Facebook* come fenomeno sociale).

Pertanto il nostro *modus vivendi* non può non subire dei mutamenti anche sotto il profilo giuridico derivante dalle responsabilità, dalla tutela e dalla violazione dei diritti che sono oggi anche i diritti della società dell'informazione. Lo stesso panorama legislativo si è contraddistinto per l'emanazione di molti provvedimenti atti a regolamentare il rapporto con le tecnologie informatiche; tuttavia si riscontra una non totale consapevolezza da parte dei soggetti, dei rischi che possono generarsi. Nel presente documento si fa riferimento ai principi contenuti nel D.Lgs. 82/2005 e nel Codice della Privacy in vista del progetto di digitalizzazione della Pubblica Amministrazione anche se è più corretto ed auspicabile dire, in vista della sua attuazione.

## CAPITOLO I

### *IL CONCETTO DI RESPONSABILITA' NEL PANORAMA DIGITALE*

In questo capitolo si vogliono riportare alcune considerazioni generali sul concetto di responsabilità al fine di fornire un valido supporto per la comprensione delle specifiche fattispecie trattate nei capitoli seguenti. Da *Wikipedia* si legge che << la *responsabilità giuridica* consiste nell'obbligo e nelle obbligazioni che si riconnettono per il compimento di atti da parte dei singoli cittadini, enti, pubbliche amministrazioni; in sostanza ogni soggetto è giuridicamente responsabile >>. Rapportando questo concetto all'interno del tema trattato, un primo quesito che emerge è quello di capire quali siano i caratteri di questa *responsabilità* ?

Volendo usare una metafora in sintonia con la tematica digitale si potrebbe affermare che tale concetto è "tridimensionale" perché ? Perché poliedrico è il contesto da cui trae origine, contesto identificato nella parola << Sistema >>. Galileo Galilei definiva sistema una pluralità di elementi materiali coordinati tra loro in modo da formare un complesso organico soggetto a regole; definizione valida anche nei nostri giorni.

La responsabilità oggetto di questa analisi deriva dalle azioni che l'individuo pone in essere all'interno di un *sistema informativo* appartenente sia ad un ente pubblico che ad uno privato. Tale sistema comprende l'insieme delle risorse umane, tecnologiche e degli strumenti propri di ciascuna realtà. Lo stesso Codice dell'Amministrazione Digitale applica l'innovativo concetto della *cooperazione applicativa*, cioè dell'interazione tra i sistemi informatici delle pubbliche amministrazioni per consentire l'integrazione delle informazioni e lo svolgimento dei procedimenti amministrativi. Pertanto si evince come il legislatore ha sancito la validità giuridica dello scambio dei documenti informatici nell'ambito di un Sistema Pubblico di Connettività (vale a dire l'insieme delle infrastrutture tecnologiche, delle regole tecniche per lo sviluppo, la diffusione, la condivisione del patrimonio informativo della P.A.). Alla luce di queste considerazioni, si delinea, dunque, un concetto di *responsabilità* a vari livelli che coinvolge sia differenti soggetti che lo stesso contesto strutturale rappresentato dal *sistema.* E' importante andare a capire quando "entra in gioco" questa *responsabilità*. Partendo dal presupposto che ognuno di noi è responsabile quando compie un'azione in maniera diligente rispettando il proprio ambito di competenza senza ledere gli interessi altrui, ne consegue che, nello scenario dei diritti delle "azioni digitali", la persona è responsabile ogniqualvolta tutela l'informazione anche mediante l'attuazione di misure preventive. L'informazione è la matrice comune alle varie situazioni; ovviamente essa assume qui un significato ben diverso dal tradizionale che comprende: il dato nelle sue qualifiche comune-sensibile-giudiziario; le modalità di

comunicazione; i soggetti destinatari. Lo stretto legame con le modalità di comunicazione sempre più interattive ha influito sul *modus operandi* anticipando, in alcuni casi, la determinazione degli effetti al momento iniziale del compimento di un'azione, al fine di poter ridurre i rischi potenziali. Infatti non bisogna dimenticare che la prospettiva di analisi dell'*Information Technology* è fortemente dinamica, ma, al tempo stesso, è caratterizzata da un indice di sicurezza che non può essere mai assoluto. A tal proposito si nota come le disposizioni contenute sia nel C.A.D. che nel Codice della Privacy stabiliscono un'inversione dell'onere di prova per dimostrare la non colpevolezza.

Altro aspetto da approfondire è il coinvolgimento di diversi soggetti attori di una determinata fattispecie, ciascuno con la propria *responsabilità.* E' il Codice della *Privacy*, a cui lo stesso C.A.D. rimanda, che per primo pone l'obbligo di identificare delle figure precise con definiti ambiti di responsabilità dirette ed indirette evidenziando, in questo modo, la necessità di avere un'organizzazione dei ruoli, una pianificazione dei compiti tra gli operatori da realizzarsi anche mediante l'attuazione di Disciplinari Aziendali, Codici Etici, Codici di Comportamento.

Alla luce di quanto appena affermato, nasce ***il Responsabile Privacy*** che può essere interno oppure esterno all'ente ed identificato quale persona fisica o giuridica preposta dal titolare alla gestione ed al coordinamento del sistema *privacy* aziendale. La designazione deve essere fatta tra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del rispetto delle disposizioni in materia di trattamento dei dati compreso l'aspetto della loro sicurezza. Nel caso in cui le esigenze organizzative lo richiedano, è possibile la designazione di più soggetti responsabili anche mediante suddivisione dei compiti.

Altro ruolo importante è rappresentato ***dall'Amministratore di Sistema*** oggetto di un aggiornamento normativo con l'emanazione del Provvedimento dell'Autorità Garante Privacy in seguito della ratifica della Convenzione Europea sui crimini informatici che ha portato all'introduzione di nuovi reati nel nostro codice penale (artt. 615-ter, 640-ter, 635-bis, 635-ter, 635 quater). Normalmente con il termine *Amministratore di Sistema* si individuano in ambito informatico figure professionali preposte alla gestione, alla manutenzione di un sistema;essi sono responsabili di specifiche fasi lavorative che possono comportare elevate criticità alla protezione dei dati e alla sicurezza della rete. La designazione dei ruoli di *System-Admnistrator, Net-Admnistrator, Data-Admnistartor* deve basarsi su profili di esperienza, professionalità ed affidabilità e tale organigramma deve essere reso noto a tutti gli utenti. L'operato degli *Amministratori di Sistema* (in sigla AdS) è soggetto a verifica annuale da parte del titolare del trattamento.

Inoltre anche nel Codice dell'Amministrazione Digitale si riscontrano figure ben definite di soggetti responsabili: la nomina di un ***Responsabile del Procedimento Amministrativo*** costituisce un elemento fondamentale del Fascicolo Informatico. Le sue funzioni sono state determinate sia dalla Legge 241/90 che dalla Legge n. 82 del 2005 in base alle quali la figura del

Responsabile del Procedimento, in primo luogo, coincide con l'Unità Organizzativa responsabile dell'istruttoria, dei procedimenti nonché dell'adozione del provvedimento. Successivamente, all'interno di ogni unità organizzativa, viene individuata la persona fisica generalmente identificata nel dirigente di quel ufficio oppure con un altro dipendente da questi espressamente individuato. *Il Responsabile del Procedimento* è colui che coordina, dirige, organizza l'istruttoria, che si rapporta con gli interessati, che cura le comunicazioni, le pubblicazioni e le notificazioni, che propone o indice la Conferenza dei Servizi.

Il processo di digitalizzazione ha portato alla nascita del ***Responsabile della Conservazione*** il cui ruolo è rinvenibile nell'art 5 della Delibera CNIPA n. 11/2004 " Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali".

*Il Responsabile della Conservazione* può essere definito come la persona fisica o giuridica, pubblica o privata a cui viene affidata la supervisione, la gestione ed il controllo del sistema di conservazione sostitutiva dei documenti. Si può desumere che data la varietà di compiti è preferibile che sia in possesso di taluni requisiti: competenze legali, tributarie, informatiche; conoscenza della disciplina del documento informatico, della fatturazione elettronica; esperienze nella fase di auditing; conoscenza dei processi organizzativi ed amministrativi e dei sistemi informativi aziendali.

Da questa prima trattazione è facilmente riscontrabile la volontà del legislatore di istituire soggetti responsabili e questo può essere letto quale fattore di garanzia dei diritti fondamentali alla luce del dettato costituzionale dell'art. 41 <<L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi, i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali>>. Tale linea di principio continua ad essere seguita anche nella recente modifica al C.A.D. in quanto le amministrazioni saranno tenute ad individuare un unico ufficio responsabile dell'attività *ICT* con conseguente distribuzione dei compiti tra i soggetti preposti.

Accanto ad una *responsabilità di ruoli* i nuovi scenari del "diritto digitale" hanno delineato e continuano a delineare specifiche fattispecie giuridiche caratterizzate da gradi differenti di *responsabilità* sia di natura civile che penale.

Nei capitoli successivi verranno esaminate alcune situazioni in cui il concetto sopra esposto deve essere desunto quale conseguenza diretta del mancato rispetto dei doveri sanciti dal Codice della Privacy e dai Provvedimenti dell'Autorità Garante del Trattamento Dati accanto ai principi contenuti nel Codice dell'Amministrazione Digitale.

## CAPITOLO II

### *SICUREZZA DATI E RESPONSABILITA'*

Nel presente contesto il concetto di sicurezza dei dati ingloba anche quello di sicurezza del documento informatico e, nel breve *excursus* normativo di seguito riportato, si vuole evidenziare come esso rappresenti uno dei principali e fondamentali elementi richiamato da entrambi i codici.
L'articolo 51, comma 2 del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale) afferma <<i documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, di perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta>> e contestualmente, l'articolo 17, lettera a) della medesima legge attribuisce il compito alle pubbliche amministrazioni di individuare un centro di competenza per il coordinamento e il monitoraggio della sicurezza informatica. A quest'ultimo articolo si ricollega anche l'Autorità Garante della *Privacy* mediante il parere emanato il 24 giugno 2010 relativo alle modifiche ed integrazioni al C.A.D. dove si afferma la necessità di prendere quale parametro di riferimento per le attività di pianificazione, coordinamento e monitoraggio, le disposizioni di cui all'Allegato B del Codice in materia di trattamento dei dati personali.
Appare, dunque, evidente come l'attuazione della sicurezza del dato/documento deriva dal porre in essere talune azioni preventive ed eventuali azioni correttive (queste ultime frutto di una costante attività di vigilanza) entrambe finalizzate al contrasto dei rischi.
Si è fatto riferimento, ad esempio, alla necessità di eliminare o almeno ridurre sensibilmente il pericolo di perdita delle informazioni.
Analizzando in dettaglio questo esempio, si può notare che in base al contesto in cui ciascun titolare opera, molteplici possono essere le soluzioni idonee da attuare. Pertanto nel caso di trattamento con strumenti elettronici, è dovere di ciascun titolare e successivamente dei soggetti da questi identificati quali responsabili ed incaricati, il programmare un'idonea procedura di *back-up* accanto ad una puntuale operazione di manutenzione e conservazione degli strumenti elettronici, dei supporti di copia e della stessa rete.
Invece, per quanto riguarda il pericolo di "accesso non autorizzato" è fondamentale attribuire ai vari utenti incaricati le proprie credenziali di autenticazione caratterizzate da un alto grado di riservatezza ed è fondamentale attribuire dei profili personali di autorizzazione in modo da limitare l'accesso ai soli dati necessari per consentire le operazioni di trattamento.

Un altro elemento di riduzione del rischio in oggetto è rappresentato dall'installazione nel sistema di specifiche soluzioni sia di tipo *hardware* che *software* atte a filtrare, a bloccare e, quindi, ad impedire le intrusioni esterne.
Non esiste un elenco omogeneo di soluzioni da seguire per garantire la sicurezza, ma sussiste solo l'obbligo di adottare talune misure idonee e preventive.
L'idoneità è un concetto variabile in quanto è rapportata ad ambiti operativi non identici proprio perché le variabili sono diverse. La parola variabile attiene alla tipologia del dato/documento trattato; agli strumenti elettronici utilizzati; alle caratteristiche del sistema; alle finalità di elaborazione e conservazione del dato/documento; all'ambiente; ai *software* utilizzati; alle risorse umane ed economiche impiegate.
In sintesi, dunque, la sicurezza del dato/documento è essenzialmente fondata:

a) sulla riduzione del rischio informatico;
b) sul dovere di custodia e controllo.

Qual è la responsabilità collegata ?
Il titolare del trattamento è civilmente responsabile qualora non adotta le misure di sicurezza idonee e preventive atte a ridurre al minimo i rischi.
L'articolo 15 del Codice della *Privacy* (D.Lgs. 196/2003) collega l'attività di trattamento dei dati alla disciplina della responsabilità civile applicabile alle attività pericolose attraverso il richiamo all'art. 2050 del codice civile. Pertanto l'onere di dimostrare di aver adottato le misure idonee ad evitare il danno grava sul titolare dell'attività.
Su questo tema la dottrina maggioritaria sostiene che si tratterebbe di responsabilità oggettiva in quanto è compito del gestore il dimostrare le azioni attuate che, secondo il criterio della normale diligenza, apparivano consigliabili; dunque l'unica prova liberatoria ammessa sarebbe quella del caso fortuito.
La Cassazione, invece, sostiene che non è sufficiente la prova negativa di non aver commesso alcuna violazione di legge, ma occorre quella positiva di aver impiegato ogni cura per impedire il verificarsi di un evento dannoso. In questo caso l'effetto liberatorio si può produrre se non sussiste il nesso causale tra l'attività pericolosa e l'evento.
Tuttavia nel quadro dei più generali obblighi di sicurezza, ogni titolare di trattamento deve, comunque, procedere all'attuazione delle misure definite *minime* in quanto atte a garantire almeno un livello minimale di protezione del dato/documento.
La differenza tra questa tipologia e la precedente consiste nel fatto che le "misure minime" sono specificatamente individuate nel Disciplinare Tecnico-Allegato B del Codice della Privacy.
Il Garante per la protezione dei dati personali ha sancito la sussistenza di una responsabilità penale per la mancata adozione delle misure minime di sicurezza.

Si tratta di un reato omissivo proprio della fattispecie che si perfeziona anche quando l'evento dannoso non si sia verificato. Responsabili sono i soggetti tenuti ad attivarsi per adottare le misure di sicurezza: primo fra tutti è il titolare poiché formalmente obbligato ad adoperarsi per predisporre le azioni di sicurezza e,comunque, tenuto ad operare anche in base ad una "responsabilità in vigilando".

Egli, infatti, deve scegliere i soggetti responsabili tra persone dotate di capacità, di esperienza ed affidabilità accanto al dovere di controllare l'osservanza delle norme di legge e dei programmi di attuazione definiti.

Inoltre, sono chiamati a rispondere penalmente anche eventuali soggetti definiti *responsabili* e *incaricati* quando omettono di adempiere alle istruzioni date dal titolare nei limiti delle proprie competenze e del proprio raggio di azione, ovviamente, sempre che queste istruzioni siano state formalizzate in atti scritti.

Ad esempio, il recente Provvedimento del Garante *Privacy* sugli Amministratori di Sistema (citato nel Capitolo 1) individua e determina in maniera precisa gli ambiti di operatività all'interno dei quali ciascuno è responsabile di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla  protezione del dato/documento.

## CAPITOLO III

### *FIRMA DIGITALE E RESPONSABILITA'*

La firma digitale è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica ed una privata correlate tra loro che consente al titolare tramite la chiave privata ed 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, nonché eventualmente il momento dell'apposizione della firma medesima.

Per una migliore comprensione del concetto sopra esposto è necessario procedere con la menzione di queste tre definizioni:

a) *Firma Elettronica (art.1, comma 1 lettera q- D.Lgs. 82/2005)* << l'insieme dei dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati come metodo di identificazione informatica >>;

b) *Firma Elettronica Avanzata (art.2, comma 2 Direttiva UE n. 1999/93)* << la firma elettronica ottenuta attraverso una procedura che: garantisce la connessione univoca al firmatario; è creata con i mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; è collegata ai dati ai quali si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati >>;

c) *Firma Elettronica Qualificata (art.1, comma 1 lettera r D.Lgs. 82/2005)* << è una firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro >>.

In relazione al concetto di *responsabilità* è importante distinguere due situazioni corrispondenti, da un lato al ruolo dei Certificatori e, dall'altro a quello di ogni titolare di firma.

La disciplina della *responsabilità del Certificatore*, identificato in colui che rilascia al pubblico un certificato qualificato, è regolamentata in vari articoli dallo stesso Codice dell'Amministrazione Digitale. D'altronde non potrebbe essere diversamente dal momento che dal suo operato scaturiscono precisi diritti altrui.

In primo luogo, egli è tenuto ad accertarsi della completezza dei dati necessari per la firma in base ai requisiti richiesti per i certificati qualificati. Il Certificatore è chiamato, altresì, a rispondere dei danni nei confronti dei terzi in caso di mancata o non tempestiva registrazione

della revoca e nel caso di non tempestiva sospensione del certificato dal cui uso possono essere sorte situazioni oggettive e soggettive di diritto.
Pertanto il certificatore è obbligato ad accertarsi dell'identificazione della persona a cui viene rilasciato il certificato ed, al contempo, è suo dovere garantire la riservatezza dei dati acquisiti. Inoltre egli è tenuto ad una precisa e corretta osservanza delle regole tecniche stabilite per la generazione e la conservazione del medesimo certificato.
L'ipotesi di una sua deresponsabilizzazione è collegata alla dimostrazione di aver agito senza dolo e senza colpa. Si ricorda che, secondo quanto disposto dall'art. 31 del D.Lgs. 82/2005, il Cnipa (oggi Digit PA.) esercita una funzione di vigilanza e controllo sull'attività dei certificatori qualificati ed accreditati.
Come è stato in precedenza rilevato, la firma digitale determina situazioni giuridiche di diritto e, pertanto, la sua detenzione ed il suo uso da parte del titolare devono avvenire con particolare cautela e con piena consapevolezza. Infatti, molto spesso, è proprio la mancanza di un'adeguata conoscenza dei pericoli indiretti che induce il firmatario a situazioni di rischio con più o meno gravi conseguenze.
Innanzitutto si mette in risalto, il riconoscimento al documento informatico sottoscritto con firma elettronica qualificata e, in particolare, con firma digitale dell'efficacia attribuita alla scrittura privata dal nostro codice civile. Al riguardo è da tempo che sta emergendo un orientamento della dottrina atto a considerare il documento informatico sottoscritto con firma digitale con una valenza maggiore rispetto alla tradizionale scrittura privata. Il motivo è dettato dalla mancanza del disconoscimento della sottoscrizione digitale. Infatti la firma apposta, seppur in modo abusivo, è sempre del titolare della chiave e, quindi, è sempre identica; per cui se il titolare del certificato smarrisce la firma o l'affida ad un altro, la sua apposizione in un documento è imputabile allo stesso autore con tutela dell'eventuale soggetto terzo che ha riposto l'affidamento in buona fede.
Alla luce di queste considerazioni giuridiche appare evidente la *responsabilità* di ciascun titolare di firma: egli è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare il danno e,quindi, è suo obbligo quello di custodire e di utilizzare il dispositivo di firma con la diligenza del buon padre di famiglia (art. 32, comma 1 D.Lgs. 82/2005). E' lo stesso titolare che deve dimostrare di aver subito una sottrazione con violenza della chiave privata, dell'eventuale malaintenzione del terzo a cui l'aveva affidata per un determinato fine. Ancora una volta si può notare come tale situazione richiami, seppur indirettamente, la responsabilità per esercizio di attività pericolosa regolamentata dall'art. 2050 del codice civile e collegata alla disciplina in materia di trattamento dei dati personali.
Tuttavia nel caso di abuso della firma, l'autore può immediatamente interrompere l'imputazione mediante l'inoltro della richiesta di revoca o di sospensione a fronte della quale il certificatore è tenuto ad assicurare la precisa determinazione della data e dell'ora di esecuzione.

In conclusione si mette in luce l'unica ipotesi in cui il firmatario non è esposto a *responsabilità* indirette: nel caso di apposizione della firma digitale ad un documento dinnanzi ad un notaio o ad un pubblico ufficiale autorizzato. Infatti l'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e della corrispondenza tra quanto dichiarato nel documento e quanto voluto dal soggetto.

## CAPITOLO IV

### *POSTA ELETTRONICA CERTIFICATA E RESPONSABILITA'*

La posta elettronica certificata trova anch'essa una sua collocazione all'interno del Codice dell'Amministrazione Digitale, precisamente nel Capo IV dedicato alla trasmissione informatica dei documenti; in realtà questo strumento è regolamentato dal D.P.R. n. 68 del 2005.
La funzione della posta elettronica certificata è simile alla raccomandata cartacea, ma con alcune garanzie aggiuntive rappresentate dalla possibilità di avere a disposizione il contenuto della "busta spedita" superando il limite della presunzione di conoscenza dell'attuale posta ordinaria.
Infatti tale trasmissione telematica è caratterizzata da una ricevuta di accettazione e da una ricevuta di consegna entrambe corrispondenti ad un e-mail in cui è riportata la data e l'ora di trasmissione e di ricezione di un documento.
L'importanza di un indirizzo di posta elettronica certificata è contenuta nel suo "valore legale" ossia nella capacità di produzione di effetti giuridici. A tal proposito si sottolinea che solo determinati soggetti con particolari caratteristiche possono essere riconosciuti come *Authorities* legittimate al rilascio di indirizzi a valore legale ed i loro nominativi devono essere pubblicati nel sito della DigitPA.
Lo stesso Codice dell'Amministrazione Digitale afferma che la trasmissione di un documento informatico per via telematica equivale alla notifica per mezzo della posta.
Ma quando la P.E.C. produce effetti giuridici ?
Il momento a partire dal quale inizia un eventuale conteggio temporale e comunque determina una prova per il mittente è rappresentato dalla consegna del messaggio nella casella di posta del destinatario.
Questo significa che il destinatario ha l'obbligo di controllare i messaggi ricevuti nella casella P.E.C. al fine di evitare l'insorgere di responsabilità a suo carico che potrebbero risultare anche non favorevoli allo stesso. Tale considerazione vale anche per le persone giuridiche (enti, società, professionisti) che sono obbligati a dotarsi di un indirizzo di posta elettronica certificata costituente la sede virtuale dell'attività.
Inoltre, il principio della segretezza della corrispondenza ha attuazione anche nelle trasmissioni telematiche; pertanto è vietata la consultazione non autorizzata, la duplicazione con qualsiasi mezzo e la cessione a qualsiasi titolo, anche in forma sintetica, delle informazioni oggetto di un messaggio di posta elettronica certificata.
Ne deriva, ovviamente, che ogni violazione di quanto appena esposto comporta *responsabilità* di natura penale.

E’ importante, quindi, custodire le credenziali di accesso alla posta elettronica certificata in maniera attenta ed è parimenti importante definire per iscritto i soggetti incaricati al suo uso sulla base dei principi contenuti nel Codice della Privacy.
Il grande valore della P.E.C. spesso sottovalutato in confronto alla sua facilità d’uso, viene frequentemente richiamato in questa fase di inizio della digitalizzazione dei procedimenti.
Si cita, ad esempio, la Circolare n. 12 del 2010 emanata dal Dipartimento della Funzione Pubblica inerente le modalità di presentazione della domanda di ammissione ai concorsi pubblici.
E’stata riconosciuta la validità di trasmissione della domanda di concorso mediante P.E.C.; anzi tale inoltro soddisfa sia il requisito della sottoscrizione della domanda sia quello della data di spedizione. Per quanto riguarda il primo aspetto, l’autore risulta identificato dal sistema informatico tramite le credenziali di accesso all’utenza personale di posta elettronica certificata; mentre, in merito al secondo aspetto, la Legge 2/2009 stabilisce che ogni amministrazione pubblica certifica la data e l’ora dell’invio e della ricezione delle comunicazioni e l’integrità del contenuto mediante l’uso della P.E.C.
Tutto questo rafforza ulteriormente l’analisi degli effetti e delle responsabilità oggetto del presente capitolo.

## CAPITOLO V

### *LA RESPONSABILITA' DELLA PUBBLICA AMMINISTRAZIONE NELLA GESTIONE DEL DATO NEL SITO ISTITUZIONALE*

Il sito di una Pubblica Amministrazione definito anche come "sito istituzionale" è lo strumento di lavoro mediante cui vengono effettuati i servizi ai cittadini e le attività di scambio di documenti ed informazioni con gli altri enti attivando quella cooperazione applicativa da tempo attesa. Inoltre i siti delle amministrazioni sono anche strumento di trasparenza mediante il quale i cittadini-utenti possono valutare il livello di efficienza e produttività degli uffici pubblici; esprimere loro giudizi sulla qualità dei servizi usufruiti e costituire un veicolo di aggiornamento per verificare lo stato di avanzamento delle istanze presentate. La gestione dell'informazione all'interno del sito istituzionale non può avvenire in maniera autonoma, ma deve conformarsi a regole precise che hanno il compito di bilanciare il diritto di trasparenza dell'azione pubblica verso i cittadini con la giusta tutela della riservatezza dei loro dati. Appare, dunque, chiaro che la responsabilità della pubblica amministrazione consiste nel rispettare le modalità stabilite per la comunicazione *on-line* evitando di effettuare trattamenti difformi ed eccedenti. I dati telematici devono resi accessibili ad ogni utente comprendendo in tale concetto coloro che hanno forme di disabilità. Appare evidente che l'amministrazione deve dare maggiore risalto all'aspetto dei contenuti e dell'informazione; il riferimento al concetto dell'usabilità e della semplicità di consultazione testimonia la funzione del sito quale strumento di servizio volto al soddisfacimento dei bisogni dell'utenza. Il termine "usabilità" significa che le informazioni devono essere organizzate e strutturate in maniera da garantire la massima fruibilità.

Per quanto riguarda il concetto di "accessibilità", esso è collegato alla legge 4/2004 che ha come obiettivo quello di consentire ai soggetti diversamente abili l'accesso alla "società dell'informazione". Infatti ad essere salvaguardato è il diritto di ogni individuo ad accedere a tutte le fonti di informazione ed ai servizi, compresi quelli caratterizzati dall'impiego degli strumenti informatici e telematici. L'Articolo 2 della Legge 4/2004 definisce l'*accessibilità* come la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili senza discriminazioni anche da parte di coloro che, a causa della loro disabilità, necessitano di tecnologie assistite o configurazioni particolari. A tal proposito si evidenzia che il D.P.R. 75/2005 ha previsto che DigitPA costituisse al proprio interno un elenco di persone in possesso di specifiche qualità allo scopo di valutare nel tempo l'accessibilità dei siti istituzionali. L'ottenimento di una valutazione

favorevole comporta la possibilità di inserire all'interno del sito il bollino attestante la certificazione di accessibilità.
La forma di comunicazione deve essere caratterizzata da una completezza di informazione, da un linguaggio chiaro ed affidabile, da una semplicità di consultazione e da una omogeneità ed interoperabilità. Infatti lo scopo dei dati trasmessi sui siti è quello di ottimizzare i tempi, le procedure, i costi a vantaggio degli utenti-cittadini in maniera che la richiesta di informazione venga comunicata una sola volta e possa essere, al tempo stesso, estratta, consultata da altri uffici.
Inoltre le Pubbliche Amministrazioni dovranno rendere disponibili *on-line* i moduli ed i formulari che rappresenteranno gli unici strumenti validi per l'avvio dei procedimenti amministrativi. La mancata pubblicazione è rilevante ai fini della valutazione della responsabilità dei dirigenti.
Un altro importante aspetto è quello relativo alle modalità di trattamento da parte della Pubblica Amministrazione dei dati personali sensibili e giudiziari in conformità ai principi emanati dall'Autorità Garante *Privacy*. L'articolo 4 del D.Lgs. 196/2003 (Codice della Privacy) definisce "dato sensibile" << i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico, sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale>>; e definisce "dato giudiziario"<< i dati personali idonei a rivelare provvedimenti di cui all'art 3, comma1, lettera da a) a o) e da r) a u) del D.P.R. 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale>>.
Come già in passato è stato più volte affermato anche dalla stessa Autorità Garante della Privacy non esiste incompatibilità tra il dovere di trasparenza della Pubblica Amministrazione e il diritto della privacy degli individui: è importante che gli amministratori prima della diffusione di atti e documenti effettuino talune doverose valutazioni al fine di non ledere i diritti degli interessati.
Gli Enti possono trattare dati sensibili e giudiziari solo per fini istituzionali, quindi, è importante analizzare quando è possibile rendere pubblici atti e documenti, ma soprattutto le modalità da seguire, cercando di identificare gli interessati solo quando è necessario. In taluni casi si può procedere ad una pubblicazione parziale del documento (estratto o omissis) oppure oscurando i dati personali.
La Pubblica Amministrazione deve garantire l'esattezza e l'aggiornamento dei dati, ma, al tempo stresso, ha l'obbligo di garantire il diritto all'oblio dell'interessato una volta perseguite le finalità di trattamento.
Nella bozza di approvazione delle regole tecniche per la costituzione dell'Albo Pretorio on line (Legge 18 giugno 2009 n. 69) è stabilito che la pubblicazione deve avvenire limitatamente al periodo previsto dalla normativa di riferimento. Le amministrazioni possono stabilire tempi di

permanenza dei documenti sul sito informatico oltre il periodo di pubblicazione nel rispetto dei principi di necessità, indispensabilità, pertinenza e non eccedenza. In riferimento alla correttezza della modalità adottata, del rispetto dei tempi, all'integrità e all'intelligibilità dei documenti pubblicati ogni amministrazione individua, poi, le responsabilità dei dirigenti o dei loro delegati.
Elemento fondamentale inerente le attività di gestione del dato è rappresentato dal dovere da parte della Pubblica Amministrazione di fornire all'interno del sito istituzionale un'informativa chiara e completa in merito alle informazioni contenute, alle modalità di trattamento ed alle relative finalità.
E' infatti responsabilità dell'Ente il fornire mediante pubblicazione sul sito istituzionale i punti di seguito descritti:

a) gli scopi di rilevante interesse pubblico perseguito
b) le modalità con cui vengono gestite le informazioni ed i servizi
c) i principi di sicurezza applicati
d) le tipologie di dati trattati
e) eventuali soggetti responsabili ed incaricati
f) le operazioni eseguite ( ad esempio l'interconnessione, il raffronto, la comunicazione etc.)

In ogni caso non può mancare la possibilità per il soggetto di esercitare i propri diritti così come disposto dall'art 7 del D. Lgs. 196/2003.

Inoltre devono essere illustrati i principi di sicurezza presenti nel sito al fine di tutelare i diritti di navigazione degli utenti.

In una sezione chiamata "note legali" devono essere fornite informazioni sui seguenti argomenti:

a) copyright (possibilità e limitazioni in ordine all'utilizzo dei contenuti del sito). In questo contesto va menzionata anche l'eventuale tutela del "logo" a seguito della recente riforma del Codice della Proprietà Industriale ( D.Lgs. 131/2010) che ha dato la possibilità ai Comuni di ottenere il riconoscimento di un marchio da utilizzare per valorizzare commercialmente il patrimonio culturale, storico, architettonico ed ambientale del proprio territorio.
b) le responsabilità derivanti dall'uso del sito
c) le responsabilità sui contenuti di siti esterni eventualmente collegati
d) le regole per l'utilizzo dei documenti scaricabili dal sito

Il responsabile del procedimento di pubblicazione è individuato tra i dipendenti dell'amministrazione e, nel caso non sia espressamente nominato, è il vertice della struttura organizzativa dell'amministrazione che ne assume automaticamente la funzione. Per le finalità

del ruolo è preferibile che sia scelto tra il personale coinvolto nel processo di produzione dei contenuti ed in grado di risalire agevolmente alla fonte per ogni necessità di intervento.
Rispetto alla normativa precedente il Codice dell'Amministrazione Digitale conferma, dunque, la compatibilità delle disposizioni sull'accesso ai documenti amministrativi con quelle in materia di protezione dei dati personali.
Per ciò che concerne i limiti al diritto di accesso nel caso in cui i documenti amministrativi oggetto della richiesta di accesso contengono dati attinenti la salute e la vita sessuale, il Codice della Privacy dispone che l'interesse a visionare l'atto diventa prioritario rispetto al diritto alla riservatezza se gli interessi dei contendenti sono di "pari rango" o se l'interesse consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile. L'autorità Garante *Privacy* ha utilizzato quale elemento di raffronto per il bilanciamento di interessi non già il diritto alla tutela giurisdizionale che pure è costituzionalmente garantito, bensì il diritto soggettivo che si intende far valere sulla base del materiale documentale di cui si vorrebbe avere conoscenza. Un'eccezione alla tesi sopra descritta è rappresentata dagli elaborati concorsuali dove la riservatezza delle prove non può essere ritenuta prevalente rispetto all'esigenza della difesa di interessi giuridici.
La giurisprudenza amministrativa ha introdotto un principio di pertinenza in base al quale l'accesso agli atti di una procedura concorsuale è consentito previa garanzia dell'anonimato degli altri concorrenti. Questo si ottiene mediante l'attuazione di idonee procedure informatiche, come ad esempio, la creazione di aree riservate di accesso sul sito istituzionale a cui ogni utente è abilitato in base a proprie credenziali; generalmente per maggiore sicurezza, in caso perdita delle password, le stesse non vengono riemesse, ma sono attribuiti nuovi codici.
Il Codice dell'Amministrazione Digitale permette la possibilità di usufruire dei servizi in rete delle pubbliche amministrazioni mediante identificazione con la Carta di Identità Elettronica o con la Carta Nazionale dei Servizi.
Su questo tema era intervenuta in passato l'Autorità Garante della *Privacy* precisando che il dovere della Pubblica Amministrazione di inserire in tali carte elettroniche solo le informazioni indispensabili al riconoscimento dell'identità del cittadino. In particolare, per quanto attiene ai dati quali il gruppo sanguigno, i dati di carattere sanitario, le impronte digitali e biometriche, il Garante *Privacy* ha affermato che è dovere di ogni amministrazione che rilascia il documento, specificare quando l'interessato può non richiedere il loro inserimento nella carta o opporsi in tal senso.
Per quanto riguarda la consultazione da parte di un'amministrazione dei dati di un'altra in ottemperanza al principio della fruibilità dell'informazione, il Garante *Privacy* ha stabilito che, ai fini del rispetto della riservatezza, è importante che l'accesso avvenga solo per quelle informazioni indispensabili al perseguimento delle finalità.

La responsabilità della Pubblica Amministrazione per la gestione del dato sul sito istituzionale si manifesta anche quale dovere di controllo nei confronti di coloro che sono incaricati alla gestione e manutenzione del sito medesimo.

Da quanto finora esposto emerge l'importanza dell'attività che presiede alla realizzazione ed alla gestione del sito istituzionale. La Legge 69/2009 che ha ampliato la tipologia di dati obbligatori sul sito ed ha aumentato il rischio di sanzioni e di responsabilità gravi in caso di inadempimento.

A prescindere dalle responsabilità di tipo amministrativo e disciplinare, si evidenzia che la mancata pubblicazione delle informazioni dovute determina una responsabilità di tipo penale ai sensi dell'articolo 328 c.p. (Rifiuto di atti di ufficio. *Omissione*).

Inoltre nell'ottica dell'utente un sito istituzionale non completo o non aggiornato costituisce una violazione di diritti riconosciuti dall'ordinamento e azionabili in giudizio: basti pensare all'uso delle tecnologie nelle comunicazioni con l'amministrazione come disposto dall'articolo 3 del D.Lgs. 82/2005. Nel caso in cui un cittadino non trovi nel sito le informazioni sopra elencate, potrebbe ricorrere al giudice amministrativo per ottenere la declaratoria dell'illegittimità del comportamento dell'ente.

Inoltre la non attenzione accanto ad un non consono utilizzo dei dati, quindi, senza rispettare i principi di garanzia, trasparenza e riservatezza potrebbe esporre il responsabile a sanzioni amministrative e penali per illecito trattamento dei dati unitamente alla richiesta di risarcimento del danno in sede civile. Tale mancata attuazione potrebbe essere anche causa di responsabilità erariale: l'assenza di misure di sicurezza previste dalla normativa (D.Lgs. 196/2003) che abbiano determinato un risarcimento al soggetto leso oppure l'assenza di procedure di controllo che abbia determinato un danno diretto alle casse dell'ente e la mancata previsione nella realizzazione dei siti dell'elemento dell'accessibilità.

## CAPITOLO VI

### *CONCLUSIONI*

Più che una conclusione questo capitolo vuole essere uno spunto di riflessione su alcuni argomenti.
Un primo interessante elemento di riflessione riguarda alcune tipologie di danni risarcibili in caso di illegittime azioni o omissioni informatiche da parte della Pubblica Amministrazione. E' possibile che la Pubblica Amministrazione commetta un errore nella trasmissione di documenti per via informatica pregiudicando un diritto già acquisito di un privato. E' evidente che essa sarà tenuta a reintegrare il patrimonio del soggetto danneggiato per tutte le diminuzioni subite sia sotto l'aspetto del mancato guadagno che sotto quello delle perdite.
Un'altra ipotesi di danno patrimoniale si identifica con il fatto di pregiudicare la possibilità di ottenere qualcosa; si pensi ad esempio alla mancata comunicazione dell'ammissione o di altre comunicazioni relative ad un concorso con conseguente perdita del guadagno derivante dal probabile esercizio di quella attività.
In linea con il sistema risarcitorio dettato dalla responsabilità extracontrattuale, esiste anche l'ipotesi di danno risarcibile dal soggetto leso di natura non patrimoniale ex art. 2059 cod. civ.. Esso consiste in una lesione non oggetto di una valutazione economica che le imprese, rientrando tra i soggetti titolari di diritto a pretendere l'uso delle tecnologie da parte della Pubblica Amministrazione, possono agire per il risarcimento del danno non patrimoniale.
La giurisprudenza ha affermato che sotto il profilo del sindacato giurisdizionale, l'azione amministrativa che si avvalga dell'informatica non si differenzia in alcun modo da quella ordinaria in quanto lo schema logico da applicare coincide con quello generale che assume quale strumento necessario la verificazione della conformità dell'azione e dei suoi effetti alla norma che li disciplina.
Occorre, però, precisare che per stabilire se sussista una responsabilità o meno in capo al soggetto pubblico, non è sufficiente che questi non abbia provveduto ad osservare il comportamento prescritto dalla norma giuridica rappresentato dalla propria informatizzazione, ma è necessario valutare in concreto se sia stata pregiudicata una qualche utilità economica del soggetto privato in quanto, ai fini della responsabilità, alla sola violazione della norma non consegue in automatico un diritto al risarcimento. Questo orientamento ha acquisito una maggiore valenza di recente in conseguenza del fatto che la stessa giurisprudenza sembra aver definitivamente abbandonato, sia per quanto riguarda il danno patrimoniale che per quello non patrimoniale, la teoria del "danno conseguenza" . Essa prevedeva che in caso di certe violazioni il danno doveva considerarsi in *re*

*ipsa*. La dottrina e la giurisprudenza sono conformi nel negare l'esistenza di un danno quale conseguenza automatica dell'illecito dal momento che nel nostro ordinamento non sussiste la figura del danno punitivo; per cui un evento è risarcibile se dal fatto ne è derivata una diminuzione patrimoniale o non, che è onere del danneggiato provare.
Analogo discorso trova il suo fondamento nella prova della sussistenza dell'elemento soggettivo del dolo o della colpa in capo alla Pubblica Amministrazione, per cui questi elementi vanno verificati attraverso la prova della violazione delle regole di imparzialità, correttezza e buona amministrazione. Per la Cassazione S.U. luglio 1999 n. 500 la risarcibilità degli interessi legittimi dipende dall'accertamento dell'effettività del danno, dall'esistenza di un nesso causale tra l'evento ed il comportamento illegittimo della Pubblica Amministrazione e dalla sussistenza di una componente di dolo o colpa non del funzionario, ma dell'amministrazione-apparato che va verificata dal giudice.
Pertanto alla luce dei principi finora esposti, la violazione degli articoli 3 (Diritto all'uso delle tecnologie), 5 (Effettuazione dei pagamenti con modalità informatiche) e 6 (Utilizzo della posta elettronica certificata) del Codice dell'Amministrazione Digitale, pur costituendo un comportamento illegittimo da parte della Pubblica Amministrazione, non è ancora di per sé sufficiente a configurare una responsabilità risarcitoria in capo alla stessa essendo necessario che l'attività illecita arrechi un danno all'utente.
Infatti anche se l'amministrazione viola il diritto del cittadino alla comunicazione informatica o all'uso della posta elettronica certificata, ma con gli strumenti ordinari permette al privato di raggiungere il risultato che sta alla base dell'instaurato rapporto tra questi e l'ente pubblico, egli non subisce alcun pregiudizio dalla violazione delle norme con la conseguenza che non si può esperire l'azione risarcitoria mancando il presupposto del danno.
Il problema della giurisdizione a giudicare sulle azioni risarcitorie proposte per violazione delle norme contenute nel Codice dell'Amministrazione Digitale è stato affrontato e risolto dallo stesso testo normativo, il quale stabilisce che le controversie concernenti il diritto all'uso delle tecnologie sono devolute alla giurisdizione esclusiva del giudice amministrativo. In proposito appare importante sottolineare l'affermazione della dottrina secondo cui tale scelta risulta essere opportuna e consente di dissipare eventuali dubbi interpretativi in ordine ad un profilo delicato come è appunto quello della giurisdizione.
Pertanto indipendentemente dalla qualificazione in termini di diritto soggettivo o di interesse legittimo del diritto, i cittadini e le imprese possono adire la giustizia amministrativa per tutelarlo, tutela che per essere effettiva deve comprendere anche il profilo risarcitorio.

Un altro interessante spunto di riflessione che emerge dai temi trattati in questa relazione è la nascita di un nuovo diritto spesso identificato come *digital-law*. Questo diritto prende origine dai principi del nostro *ius* seppur se ne differenzia proprio perché diverso è il contesto in cui opera.

In particolare l'aspetto che risalta è la contrapposizione tra la rigidità, la complessità del diritto ordinario, del diritto cartaceo in confronto con la dinamicità, la flessibilità del diritto digitale.
Questa situazione influisce anche nel *modus operandi* di tutti gli operatori del diritto. Infatti la gestione di una controversia informatica necessita ormai della collaborazione anche di esperti tecnici -informatici del settore al fine di ottenere un'analisi dettagliata di ogni elemento. Non a caso è sorta al riguardo anche una specifica disciplina identificata nella *Computer Forensic* o Informatica Forense. Essa è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione ed ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche ed i mezzi per l'esame metodologico degli strumenti informatici.
Pertanto più che di una *lex romana* dobbiamo ora parlare di una "*virtual-lex*"; anche se è altrettanto interessante notare come taluni principi giuridici originati dal diritto romano, seppur con le dovute modifiche, continuano a rappresentare una fonte di regolamento.
Al tempo stesso è utile riflettere sui nuovi problemi che tale "*digital-lex*" pone al legislatore che si trova davanti a scenari prima impensabili, inimmaginabili; basti pensare al diritto all'accesso alle tecnologie informatiche, al problema della diffusione dei dati, ai problemi sociali che *internet* ha determinato, alle potenzialità dell'*e-government.*
Dall'altro lato appare ancor più urgente la necessità di una cultura dell'informatizzazione o meglio di un'educazione alla cultura che abbia come scopo sia quello di rendere maggiormente consapevoli ed efficienti gli individui nell'uso delle tecnologie sia quello di insegnare loro i limiti, i rischi che, seppur a volte non tangibili, possono essere in realtà molto gravi.
Al riguardo costituisce un aspetto interessante il  mettere in evidenzia la nascente questione del rapporto tra l'informatizzazione e l'eguaglianza sostanziale quale ulteriore elemento di prova dell'ingresso nella vita sociale delle nuove tecnologie. Come è noto il principio dell'eguaglianza sostanziale, presente nella nostra carta costituzionale, viene spesso "sostituito" dal principio dell'eguaglianza formale. Al contrario in ambito informatico esso sta acquisendo una maggiore valenza che trova riscontro nel problema della "eguaglianza digitale" la cui sottovalutazione rischia di determinare situazioni di disuguaglianza sostanziale.
E' infatti evidente che sussiste un forte *gap* tra coloro che hanno un discreto grado di istruzione informatica e coloro, in numero maggiore, che si trovano in una situazione di "analfabetismo informatico". Quest'ultimo fattore influisce nella vita sociale poiché non consente all'individuo di poter usufruire dei servizi digitali, ma soprattutto di sentirsi "non adeguato" alla realtà circostante. E' sufficiente pensare che chi non è in grado di utilizzare le tecnologie è di fatto escluso dal processo di semplificazione amministrativa in atto.
Attualmente in Italia come in altri Paesi Occidentali il divario di conoscenza ancora non è ampio (nonostante la sua continua crescita); ciò è in buona parte conseguenza del fatto che l'uso dei linguaggi e dei mezzi digitali è stato considerato come un semplice interesse personale, un

bisogno individuale privo di sviluppi collettivi. Questo concetto oggi è cambiato trasformandosi in un'esigenza della società. L'alfabetizzazione informatica si configura, quindi, come un diritto ad una prestazione sociale nel più ampio contesto del diritto all'istruzione, spettando poi al legislatore il compito di attuare le norme adeguate. E' dovere del nostro ordinamento garantire e promuovere il diritto all'istruzione rimuovendo ogni possibile ostacolo che di fatto ne impedisca lo sviluppo.

Sicuramente si è di fronte ad un compito non di facile realizzazione, almeno per il momento, in quanto esso implica alcune tematiche ed alcune problematiche diverse da quelle affrontate in passato, spesso sconosciute, con il fattore tempo caratterizzato da una rapidità e da una velocità di innovazione mai conosciuta prima. Tutto questo non deve essere affrontato con un atteggiamento di paura, di incertezza, ma, al contrario, deve far emergere quella curiosità intellettuale e quel ingegno proprio di noi italiani e fonte di "invidia" e di successo nei confronti degli altri Paesi.

In definitiva è comunque tempo che ciascuno di noi inizi concretamente ad avere "fame di sapere tecnologico" non solo per le attività ludiche, ma soprattutto per il nostro agire quotidiano da cui si originano beni e servizi collettivi; in tal modo si contribuisce alla diffusione di una sana e corretta cultura digitale al fine di creare IL SISTEMA.

***BIBLIOGRAFIA***


- Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale – Gruppo di Lavoro incaricato di una proposta di regole tecniche per l'albo on-line (Legge 18 giugno 2009,n 69 articolo 32) – anorc.it Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale – pg.5;6;7;8.

- Autorità Garante per la Protezione Dei Dati Personali - Gazzetta Ufficiale n. 170 del 23 luglio 2005 – Trattamento dei Dati sensibili nella Pubblica Amministrazione – Autorità Garante per la Protezione Dei Dati Personali –30 Giugno 2005 – pg.2;3;4;5.

- Autorità Garante per la Protezione dei Dati – Misure ed accorgimenti prescritte ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema –Autorità Garante per la Protezione Dei Dati – 27 novembre 2008 – pg. 2;3;4.

- Autorità Garante per la Protezione Dei Dati - Misure ed integrazioni al Codice dell'Amministrazione Digitale – Autorità Garante per la Protezione Dei Dati Personali – 2010 – pg.1;2;3.

- Enrico Albanesi e Paola Cappello – Sicurezza Dei Dati – Federalismi.it Rivista di Diritto Pubblico italiano, comunitario, comparato – 01 aprile 2008 – pg. 3;4;5;6;9;10;11;12;13;14;15;16;17;18;19;20.

- Elena Bassoli – E-government e Privacy – Federalismi.it Rivista di Diritto Pubblico italiano, comunitario, comparato – 10 aprile 2008 – pg. 3;4;8;9;10;11;15;20;21;22;23;24;25;26;27;28;29;30.

- Ernesto Belisario – La gestione dei siti web delle P.A. (ex art 54 cad) – Egov Maggioli – 2009.

- Prof. Ermanno Calzolaio – Volontà e imputazione della dichiarazione nel documento informatico:spunti per una riflessione – pg. 5;6;9;10;11;12.

- Francesco Camilletti – La Responsabilità della Pubblica Amministrazione per violazione del diritto all'uso delle tecnologie – Federalismi.it Rivista di Diritto Pubblico italiano, comunitario, comparato – 27 aprile 2008 – Cap. 2) pg.8;9;10; Cap 3) pg. 13;14;15.

- Giampiero Paolo Cirillo – Codice in Materia di Trattamento dei Dati Personali - Giuffrè Editore 2004 - pg.23:24;74;75;76;77;183;184;185;186;187;;188;189;190;191;253;254;255;256;257;258; 259260;261;262;263;264.

- Prof. Eugenio De Marco – Rapporto di Ricerca- Eguaglianza Digitale - Federalismi.it Rivista di Diritto Pubblico italiano, comunitario, comparato – pg.7;8;9;10;11;12;13;14;15;16;17.

- Dr. Eric Frantone – Privacy e Conservazione Sostitutiva: Responsabili a confronto – Eucs – Padova 04 Maggio 2007 – pg.5;6.

- Dott. A. Giuffrè spa - Decreto Legislativo, 07/03/2005, n. 82 Gazzetta Ufficiale 16/05/2005 n. 112 - Giuffrè Editore – pg.4;5;12;13;14;15;16;18;23;24;28;29;30;31;32;33;34.

- Daniele Marongiu – Quaderni del DAE- Rivista di Diritto Amministrativo Elettronico La trasmissione del Documento Informatico: il ruolo della posta elettronica certificata – Diritto Amministrativo Elettronico – 2005 – paragrafo 3) pg.4;5;6;7.

- Dott.ssa Anna Papa – Il Principio di Uguaglianza sostanziale nell'accesso alle tecnologie digitali - Federalismi.it Rivista di Diritto Pubblico italiano, comunitario, comparato – pg.34;35;36;37;38;39;40;41;42.

- Presidenza del Consiglio Dei Ministri- Dipartimento della Funzione Pubblica – Circolare n. 12- Procedure concorsuali ed informatizzazione. Modalità di presentazione della domanda di ammissione ai concorsi pubblici indetti dalle amministrazioni. Chiarimenti e criteri interpretativi sull'utilizzo della PEC – Presidenza del Consiglio Dei Ministri – 2010 – pg.3;4;5;6;7.