Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Specialistica in Scienze di Internet

I PRINCIPALI STRUMENTI GIURIDICI PER LO SCAMBIO DI DATI TRA LE PUBBLICHE AMMINISTRAZIONI

Tesi di Laurea in Diritto Privato Generale E Dell'Informatica

Relatore:
Prof. Giusella Finocchiaro

Presentata da:
Antonio D'Alto

Sessione I
Anno Accademico 2010/2011

Introduzione

L'avvento dell'informatica e dell'elettronica nella società ha determinato un profondo cambiamento degli assetti in ogni settore.

Per quanto riguarda la Pubblica Amministrazione, già a partire dalla metà degli anni '50 si può riscontrare l'ingresso, nell'ambito gestionale, di tecnologie basate sull'automazione di alcune attività, grazie all'utilizzo di strumenti "primordiali", come le schede perforate o i nastri. Si tratta di una prima fase che non può essere inquadrata come "informatizzazione", ma che può essere invece definita come "meccanizzazione", alla quale comunque va il merito di aver avviato un importante processo di alleggerimento del lavoro umano, di snellimento di tempi, e di velocizzazione dei processi.

La seconda fase è invece quella che ci da il diritto di parlare di informatizzazione vera e propria: è questa la fase caratterizzata dall'utilizzo di elaboratori elettronici e relativi software, grazie ai quali sono stati apportati enormi benefici a specifici settori dell'Amministrazione.

Spostando il focus sui nostri giorni, si può affermare che gli investimenti statali nel settore informatico sono costantemente cresciuti, pur rimanendo tuttavia al di sotto della media degli altri Paesi Europei.

L'utilizzo degli strumenti informatici a livello di strutture pubbliche e la progressiva diffusione delle banche dati "online" ha portato alla luce un pericolo fondamentale che rappresenta un ulteriore problema riguardante i rapporti tra amministrazione, nuove tecnologie ed utenti finali. Si vuole, in questo caso, accennare alla possibile violazione della privacy dei soggetti, a causa della natura intrinseca del mezzo, il quale può effettivamente

contribuire a rendere la nostra società "trasparente".

L'esistenza di una rete globale può permettere a chiunque l'accesso alle informazioni, ancor più nello specifico alle informazioni sensibili degli individui. Tale pericolo appare ancora più attuale quando si pensa alle metodologie applicate al fine di costruire una rete unitaria delle PA: la concezione è identica a quella che sta alla base di internet, ovvero una "rete di reti" in grado di mettere in comunicazione tra loro un numero non definito di utenti. Inoltre in una situazione del genere, si rischia di effettuare una inconsapevole discriminazione tra chi è in possesso di determinate capacità tecniche e chi no; si corre il pericolo di escludere un numero consistente di individui incapaci di rapportarsi con la tecnologia, facendo cosi sfumare l'intento di quest'ultima, ovvero la semplificazione delle procedure e lo sveltimento dei rapporti tra PA e cittadini.

La creazione di un sistema informatizzato, se supportata da una reale considerazione delle esigenze del cittadino, può contribuire alla realizzazione di una rete funzionale, la quale implica un attiva partecipazione dei soggetti. Affinchè ciò sia possibile è necessario che, nell'adeguare le strutture amministrative alle innovazioni tecnologiche, siano salvaguardati due punti fondamentali nel rapporto cittadino – PA. In primo luogo va garantito al privato l'accesso alle banche dati dell'amministrazione; in secondo luogo è indispensabile che sia previsto un obbligo per le amministrazioni di salvaguardare la segretezza delle notizie individuali, limitando di conseguenza lo scambio di informazioni tra PA, qualora la loro diffusione incida sulla riservatezza dei dati relativi alla persona. Di qui la necessità di prevedere adeguate misure di sicurezza dirette a garantire la segretezza e la riservatezza dei dati non pubblici contenuti nelle banche dati.

Si presenta dunque l'esigenza di tutela del diritto di accesso alle banche dati, da un lato, e del diritto alla riservatezza, dall'altro: entrambi possono essere condensati nel concetto di "diritto di libertà informatica". D'altro canto va sottolineato come lo stato sia tenuto, per ragioni di pubblico interesse, ad avvalersi, in particolari situazioni, delle sue capacità di informazione an-

che a discapito di riservatezza individuale. Dunque ci si trova davanti a due esigenze non facilmente compenetrabili: da una parte vi è quella del privato di vedere tutelata la sua privacy contro intrusioni esterne; dall'altra c'è la necessità dello Stato di sacrificare questa privacy tutte le volte che ragioni di interesse generale lo rendano indispensabile. Compito del Legislatore è di rendere compatibili queste esigenze, al fine di rendere lo strumento informatico un mezzo funzionale alla realizzazione dei diritti e non alla loro violazione. Lo scopo del seguente lavoro, invece, sarà quello di illustrare i mezzi utilizzati in ambito amministrativo per garantire la privacy a cui prima si faceva riferimento: stiamo parlando della PEC, ovvero della posta elettronica certificata. Inizialmente si tratteranno aspetti più tecnici legati a tale strumento, dandone una definizione e illustrando i metodi di funzionamento; successivamente si affronteranno invece aspetti legati più nel dettaglio all'ambito giuridico, discutendo dell'efficacia probatoria del documento informatico, dell'uso della firma digitale e della firma elettronica nella PEC[1], del valore giuridico delle mail, e di come si sia evoluto lo strumento dal d.p.r. n. 68/2005 al 235/2010. Per meglio comprendere gli aspetti giuridici del lavoro, si accennerà, in precedenza, un po' più nello specifico alla firma elettronica e alla firma digitale, affrontando gli aspetti tecnici che la riguardano, e gli enti certificatori legati ad essa.

Dopo aver definito gli strumenti utilizzati per garantire la sicurezza nello scambio di dati, si sposterà il focus sull'argomento, probabilmente, cardine di questo lavoro: la PEC e la privacy; si parlerà dell'indirizzo e-mail come dato personale, di come vengono elaborati e trattati i dati personali e di aspetti legati allo spamming e alle comunicazioni indesiderate.

Come già accennato in precedenza, la seconda "fase" dell'introduzione nelle PA della tecnologia prende il nome di "informatizzazione": questo processo verrà analizzato nel dettaglio, snocciolando l'utilizzo della PEC nelle PA e di come questo strumento venga usato per la notificazione degli atti.

[1]Da questo momento in poi si utilizzerà la dicitura PEC come posta elettronica certificata

In ultimo, ma non per questo di meno rilevanza, verranno trattati argomenti di carattere generale che riguardano l'e-government, inteso[2] come processo di informatizzazione della PA, il quale, unitamente ad adozioni di cambiamento organizzativo, consente di trattare la documentazione e di gestire i procedimenti con sistemi digitali, grazie all'uso di tecnologie dell'informazione e della comunicazione, allo scopo di ottimizzare il lavoro degli enti e di offrire agli utenti sia servizi più rapidi, che nuovi servizi. Bisognerà, di conseguenza, trattare aspetti legati alla sicurezza degli strumenti utilizzati, nello specifico delle metodologie e delle tecniche volte alla salvaguardia dei sistemi informatici da potenziali rischi o violazioni dei dati, alla protezione della confidenzialità, dell'integrità e della disponibilità di questi.

[2]Definizione da: www.wikipedia.org

Indice

Capitolo 1

La PEC

1.1 Definizione

La posta elettronica certificata è uno strumento che permette di dare ad un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale. La PEC può inoltre aggiungere la certificazione del contenuto del messaggio solo se in combinazione con un certificato digitale; nell'utilizzarla, nel momento in cui il mittente omette di usare la propria firma digitale, la PEC non ne certifica l'identità, ne trasforma il messaggio in "documento informatico".[urla]

Da una semplice e breve definizione vanno estrapolati e approfonditi già molteplici aspetti: cosa si intende per messaggio di posta elettronica? Quali sono le differenze con un messaggio di posta elettronica certificata? Cosa si intende per certificazione? Procediamo per passi. Un messaggio di posta elettronica "tradizionale" è la controparte digitale ed elettronica della posta ordinaria e cartacea; i messaggi di posta elettronica avvengono mediante lo scambio di parti testuali o file, attraverso una rete telematica, come per esempio internet, solitamente tra terminali o calcolatori (ma in generale tra strumenti che la supportino).

La posta elettronica rappresenta la connessione personale che un utente ha su internet e fornisce un meccanismo standard che consente di scambiare,

in modo rapido, comunicazioni private tra individui. L'analogia tra casella di posta elettronica e servizio postale è quantomai veritiera in quanto:

- le comunicazioni avvengono in modo privato
- entrambe si basano sugli stessi principi

Infatti, ogni utente possiede un proprio indirizzo e-mail che lo identifica in maniera univoca all'interno della rete. In questo modo sono possibili:

- invii di posta tra utenti mediante la specificazione dell'indirizzo
- ricezioni al proprio indirizzo di messaggi provenienti da altri utenti

A differenziare il sistema di posta elettronica, rispetto al servizio postale o anche altri tipi di comunicazioni, (come quella telefonica), ci sono alcune basilari concezioni: nella posta elettronica il sistema di comunicazione è asincrono, ovvero il mittente e il destinatario non devono sincronizzarsi temporalmente per comunicare, ma possono inviare o leggere i messaggi nel momento in cui lo ritengono più opportuno.

Nella tabella 1.1 riporto le principali differenze tra comunicazione telefonica e comunicazione via mail:

	Telefono	**Email**
Tipo di comunicazione	Sincrona	Asincrona
Documentabilità	No	Si
Stile	Elaborato	Essenziale

Tabella 1.1: didascalia

In generale i punti di forza della posta elettronica sono altri ancora: innanzitutto vi è la possibilità di inviare non solo testo, ma tipi di file di diversa natura (file audio, file video, immagini), in tempi rapidi, garantito da una velocità di trasmissione che permette di effettuare tali operazioni nell'arco di

pochi secondi. Inoltre il mezzo di trasmissione è nei limiti, (e più in avanti attribuiremo a questa frase il giusto significato) affidabile, in quanto, almeno sotto il lato della dispersione dei messaggi, risulta funzionale e ben adatto al tipo di lavoro. Infine, il mezzo è caratterizzato dai costi contenuti, tali grazie alle innumerevoli possibilità di connessione che troviamo oggigiorno, e dalla possibilità di comunicazione multipla, ovvero il poter inviare lo stesso messaggio, contemporaneamente, a più persone.

Il modello su cui si basa il servizio di posta elettronica viene definito di tipo "client-server", dove:

- server: software che risiede su un computer collegato in rete, e che, in relazione al servizio erogato, accetta richieste e invia automaticamente risposte
- client: interfaccia che fornisce l'acceso ad un server che eroga un servizio

Gli utenti per usufruire dei servizi offerti da un server di posta elettronica, devono utilizzare un particolare software, chiamato client di posta elettronica, che permette di comunicare con un server in rete.

Il servizio di posta elettronica è composto da:

- un client: ovvero un programma presente sul computer dell'utente che si occupa della gestione (in uscita e in entrata) della posta
- un server SMTP (simple mail transfer protocol) conosciuto anche come server di posta in uscita, ovvero il server a cui il client di posta si collega per inviare messaggi
- un server POP (post office protocol) conosciuto anche come server di posta in entrata, ovvero il server su cui risiede la casella di posta elettronica dell'utente in cui sono conservati i messaggi in ingresso. Il client si collega a tale server quando l'utente desidera scaricare la posta.

La comunicazione via mail dunque, avviene schematicamente come riportato in 1.1: un utente invia un messaggio, la cui correttezza e destinazione

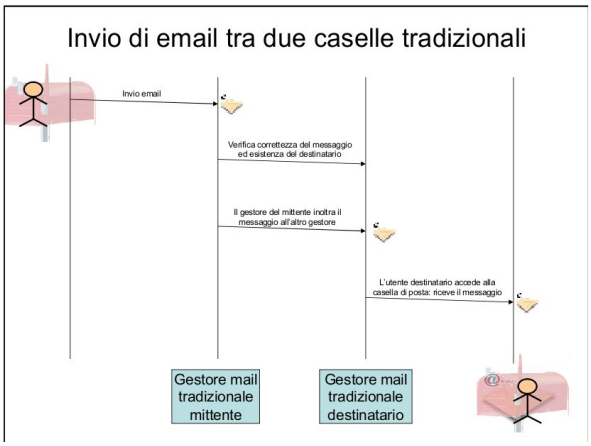

Figura 1.1: Invio di email tra due caselle tradizionali

viene verificata dal proprio gestore di mail tradizionale; successivamente il gestore del mittente inoltra il messaggio al gestore di mail del destinatario e infine quest'ultimo, accedendo alla casella di posta, ne verifica la ricezione.

Dalle seguenti operazioni derivano i seguenti interrogativi: chi ha inviato il messaggio? ovvero la verifica se è, o meno, colui che nella mail figura come mittente; a che ora è stato spedito il messaggio? Ovvero la verifica se l'orario è quello indicato nella mail; cosa voleva dirmi il mittente? Ovvero la verifica del contenuto della mail o dei relativi allegati.

Tutti questi interrogativi non trovano più ragion d'essere nella posta elettronica certificata; lavorando in quest'ambito, infatti, troveremo la combinazione di due elementi, ovvero la posta elettronica tradizionale connessa alla sicurezza e alla certificazione. Procediamo per passi. La sicurezza, in tale ambito, ci viene garantita dall'utilizzo del protocollo ssl, il quale permette ai dati di viaggiare in modo cifrato. SSL è il protocollo crittografico utilizzato per garantire la sicurezza in informatica e nelle telecomunicazioni. Creato nel 1994 da NetScape, si è subito imposto come standard per lo scambio dei dati su internet, e rappresenta, al momento, lo standard più largamente utilizzato dai servizi web per proteggere i dati da alterazioni o accessi non autorizzati.

Il protocollo SSL garantisce la sicurezza dello scambio di dati in ambiente insicuro grazie alle seguenti caratteristiche che lo contraddistinguono:

- Sicurezza
- Autenticazione
- Integrità delle informazioni scambiate

La certificazione, invece, ci viene data dall'utilizzo di ricevute, ovvero dall'accettazione e dalla consegna. La certificazione viene garantita dall'uso di un certificato digitale, ovvero un documento elettronico che attesta, mediante l'uso di firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto. In altri termini, lo scopo del certificato digitale è quello di garantire che una chiave pubblica sia associata alla vera identità del soggetto che la rivendica come propria.

Una trasmissione può essere considerata "posta certificata" solo se le caselle del mittente e del destinatario sono entrambe caselle di posta elettronica certificata, altrimenti il sistema potrà fornire solo una parte delle funzionalità di certificazione previste.

Le principali caratteristiche della PEC in generale sono:

- accesso e identificazione: L'utilizzo dei servizi di posta certificata avviene esclusivamente utilizzando protocolli sicuri, in modo da evitare qualsiasi manomissione del messaggio e degli eventuali allegati da parte di terzi. Infatti tutte le comunicazioni sono protette perché crittografate e firmate digitalmente. La maggior parte degli strumenti di posta più diffusi sono già in grado da tempo di gestire protocolli per comunicazioni "sicure" (come HTTPS, SMTPS, POP3S, IMAPS). L'identificazione solitamente avviene tramite l'uso di tecniche consolidate, come il sistema username/password, oppure tramite certificati digitali. La falsificazione d'identità viene invece combattuta grazie alla possibilità di inserire nella casella "from" solo ed esclusivamente il proprio indirizzo email, contrariamente a quanto avviene nei server di posta in internet, dove si può cambiare la casella mittente con estrema facilità

- Integrità del messaggio : A completa garanzia dell'integrità del messaggio, mittente e destinatario sono obbligati a utilizzare la casella PEC solo tramite protocolli sicuri, come descritto in precedenza

- Certificazione dell'invio : Quando si invia un messaggio da una casella PEC si riceve dal proprio provider di posta certificata una ricevuta di accettazione che attesta la data e l'ora della spedizione ed i destinatari.

- Certificazione della consegna : Il provider del destinatario invia al mittente la ricevuta di consegna. Anche in questo caso si tratta di un messaggio e-mail che attesta:

    1. la consegna con l'indicazione della data e ora la consegna con l'indicazione della data e ora
    2. contenuto consegnato

Questo ultimo punto va particolarmente sottolineato, in quanto la ricevuta di consegna contiene, in allegato, anche il messaggio vero e proprio. Questo significa che la posta elettronica certificata fornisce al mittente una prova di tutto il contenuto che è stato recapitato. Questa è una delle caratteristiche più significative che contraddistingue la PEC dai normali mezzi per l'invio di documenti ufficiali in formato cartaceo.

Bisogna inoltre accennare agli obblighi dei gestori in ambito della PEC: questi devono garantire la registrazione di tutti i principali eventi che riguardano la trasmissione per 30 mesi, da fornire come prova da parte degli interessati; inoltre è previsto un allineamento orario con istituti ufficiali, che garantisca stabilmente uno scarto non superiore al secondo rispetto alla scala di Tempo Universale Coordinato (ora coordinata in tutto il mondo con il meridiano di Greenwich). Oltre ai principali obblighi prima accennati ,il gestore inoltre deve:

- garantire i livelli di servizio previsti

- assicurare l'interoperabilità con altri Gestori accreditati

- fornire al mittente la ricevuta di presa in carico, accettazione e di avvenuta consegna del messaggio di posta elettronica certificata
- comunicare al Titolare della casella di posta elettronica certificata la mancata consegna del messaggio entro le 24 ore dall'invio
- effettuare la corretta trasmissione dal mittente al destinatario conservando l'integrità del messaggio originale nella relativa busta di trasporto
- agire nel rispetto delle norme previste dal Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali
- effettuare la disattivazione di una casella PEC dopo aver verificato l'autenticità della richiesta
- utilizzare dispositivi di firma conformi con la normativa

Da CNIPA: La posta elettronica certificata, (Supp. Al n. 1/2007 del periodico innovazione): "Vantaggi della Pec

- certificazione dell'avvenuta consegna del messaggio nella casella di posta del destinatario del messaggio e dei suoi contenuti
- certificazione degli allegati del messaggio
- possibilità di allegare al messaggio qualsiasi tipologia di informazione e/o documento in formato digitale
- archiviazione da parte del gestore di tutti gli eventi (certificati) associati ad invii e ricezioni, per un periodo di 30 mesi
- semplicità di trasmissione, inoltro, riproduzione, archiviazione e ricerca dei messaggi
- economicità di trasmissione, inoltro, riproduzione, archiviazione e facilità di ricerca

- possibilità di invio multiplo, ovvero a più destinatari contemporaneamente (e verosimilmente con costi molto più bassi rispetto a quelli delle raccomandate)
- tracciabilità della casella mittente e quindi del suo titolare
- velocità della consegna (ma soprattutto del ricevimento delle ricevute)
- elevati requisiti di qualità e continuità del servizio
- applicazione delle procedure atte a garantire la privacy dei dati personali, nonché la sicurezza
- garanzia dell'identità del mittente (titolare della casella).

Svantaggi della Pec

- conoscenza effettiva del messaggio sostituita da conoscibilità (valore di presunzione di conoscenza)
    1. 1)tale effetto è proprio della CEC-PAC[1] (notifica a mezzo postale) e della CPEPCT[2], non ancora della PEC
    2. 2)in ogni caso, la PEC ci avverte solo se non arriva dal mittente al proprio gestore, o dal proprio gestore al gestore del destinatario, ma non ci avverte se il destinatario l'ha letta effettivamente
- la PEC non è standard internazionale, in quanto insieme di regole tecniche e giuridiche proprie solo dell'Italia

[1] CEC-PAC è tecnicamente l'acronimo di "Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino" Ne da una prima forma regolamentativa il Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009, pubblicato sulla G.U. il 25 Maggio 2009, che stabilisce le disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini. Seguito poi nel dettaglio dal Bando per l'affidamento in concessione del "servizio di comunicazione elettronica certificata tra pubblica amministrazione e cittadino (CEC-PAC)" mediante procedura ristretta.

[2] Casella di posta elettronica certificata del processo telematico

- la normativa non è conforme alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 (in G.U.C.E. L. 13 del 13 dicembre 1999) Relativa ad un quadro comunitario per le firme elettroniche
- i requisiti richiesti dalla legge per poter diventare gestore, sono talmente gravosi da escludere di fatto dal mercato i piccoli operatori, facendo cosi in modo che i costi non sono il risultato di una concorrenza effettiva
- costi dell'hardware
- digital divide geografico, sociale ed economico
- nuovi diversi problemi di privacy e deontologia
- altri nostri dati personali viaggiano in rete e vengono trattati da terzi, PA inclusa, esponendo la nostra privacy ad altre nuove sollecitazioni e rischi come:
  1. spamming
  2. furto d'identità
  3. phishing
  4. furto di dati
- rischi per la segretezza della corrispondenza elettronica:
  1. i dati personali e le informazioni viaggiano in protocolli sicuri ma risiedono in chiaro nelle caselle
  2. i dati personali e le informazioni sono backuppate dai gestori (come? Da chi? Per quanto tempo?)
  3. equivalenza a divulgazione dei dati personali e delle informazioni
  4. diffusione di strumenti di crittografia e/o steganografia
- impatto ambientale per ogni messaggio inviato, anche di errore:

1. da stampa su carta del "traffico" generato: almeno 6 fogli per ogni mail via PEC, dati da messaggio, firme digitali, ricevute
2. 2) da aumento del traffico nella rete, dovuto all'impegno di risorse di storage, impegno della banda (che come sappiamo in Italia non sempre è larga), impegno energetico.

L'utilizzo della PEC assume un utilizzo sempre più esteso nei rapporti tra PA e privati, soprattutto imprese. Viene considerata lo strumento ottimale per le comunicazioni un tempo affidato alla carta bollata ed il suo utilizzo è sempre più diffuso anche per consentire il contenimento dei costi ed un miglioramento dell'efficienza e dell'efficacia della attività da parte della PA.

La normativa recente, soprattutto quella per l'avvio di un impresa in un giorno, ha praticamente assegnato una PEC ad ogni impresa con l'intento dichiarato di rendere più veloci le comunicazioni relative alla vita delle Pmi[3] ma ulteriori scenari sembrano aprirsi nell'utilizzo di questo strumento. Il successo della Posta Elettronica Certificata è sostanzialmente dato dalla "garanzia" della trasmissione del documento dal mittente al destinatario: non ci sono più plichi e comunicazioni che si perdono lungo il tragitto. La garanzia della trasmissione (e della ricezione) ha un valore legale pari a quello un tempo affidato alle raccomandate.

Le comunicazioni effettuate tramite PEC, dunque, hanno un valore superiore rispetto alla tradizionale mail di posta elettronica.

La manovra correttiva[4],[CNI10] pubblicata il 31 maggio, ha reso consultabili gli elenchi contenenti gli indirizzi PEC non solo dal personale della Pubblica Amministrazione, ma anche dagli agenti della riscossione. L'amministrazione e le Pmi scambieranno quindi più velocemente ed efficacemente i

[3]Da questo momento con PMI si intende piccola e media impresa

[4]E' in vigore dal 31 maggio il decreto legge "recante misure urgenti in materia di stabilizzazione finanziaria e di competitività economica". Il provvedimento è stato pubblicato sulla Gazzetta Ufficiale Serie Generale n. 125 del 31 maggio 2010, Supplemento ordinario n. 144. Il decreto-legge, meglio noto come manovra finanziaria correttiva, è stato firmato dal Presidente della Repubblica e si compone di 56 articoli più allegati.

propri atti tramite la PEC ma altrettanto veloci ed efficaci saranno le notifiche effettuate ad esempio dall'INPS per il recupero dei crediti in concomitanza con il previsto incremento delle attività di controllo automatizzate (leggi incrocio dei dati tra INPS e Agenzia delle Entrate) ed alla velocizzazione delle procedure di riscossione.

Nella PEC arriveranno, quindi, anche le cartelle di pagamento che, al momento della consegna all'indirizzo certificato e a prescindere dall'avvenuta lettura da parte del contribuente, avranno il valore di "notifica eseguita".

La tecnologia aumenta le possibilità di fare, ed in questo caso le imprese dovranno fare molta attenzione e soprattutto considerare la casella della PEC un ulteriore, importante, canale di comunicazione con la PA che va costantemente tenuto d'occhio evitando sviste su atti fondamentali.

1.2 Specifiche di funzionamento

In figura 2 è riportato un esempio di comunicazione tramite PEC: al momento di un invio di una mail, il gestore PEC si occuperà di inviare al mittente una ricevuta, la quale ha il valore legale dell'avvenuta o mancata trasmissione del messaggio, con precisa indicazione temporale del momento in cui la mail PEC è stata inviata. Il gestore del destinatario, depositato il messaggio PEC nella casella di proprietà, fornisce al mittente una ricevuta di avvenuta consegna, con l'indicazione temporale nel quale tale consegna è avvenuta.

La certificazione della consegna avviene tramite il seguente passaggio: un messaggio di posta certificata viene consegnato nella casella del destinatario inserito nella sua busta di trasporto; nel momento in cui viene effettuata la consegna, il provider del destinatario invia al mittente la ricevuta di consegna, cioè un messaggio email "firmato" dal gestore che attesta la consegna, la data e l'ora di consegna, il contenuto consegnato. La PEC fornisce al mittente una prova di tutto il contenuto che è stato recapitato, e questa è una delle caratteristiche più significative che distingue la posta certificata dai normali

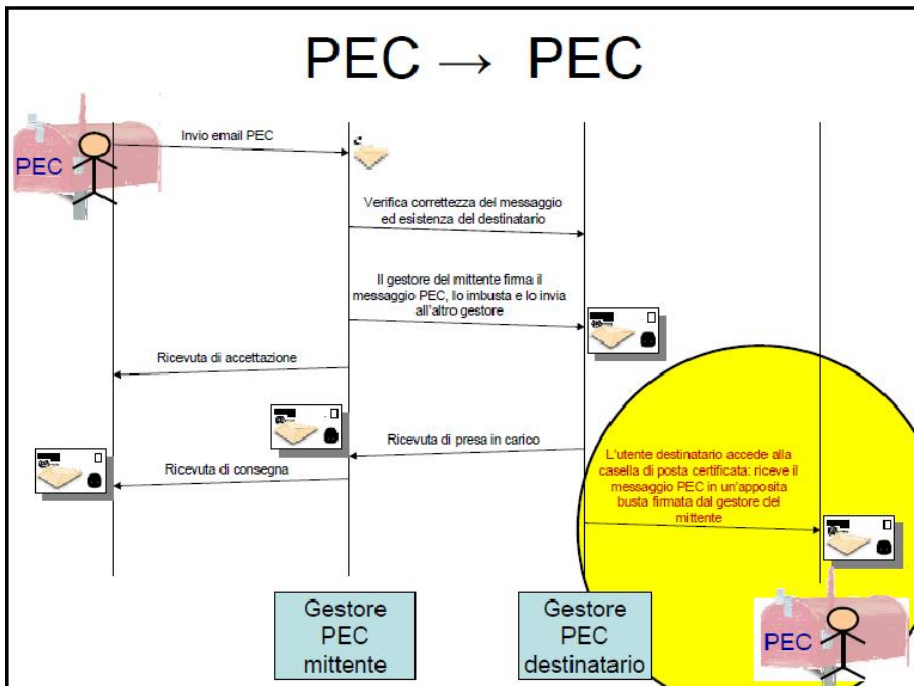

Figura 1.2: Invio e ricezione di messaggi tramite PEC

mezzi per l'invio di documenti ufficiali in formato cartaceo. Il gestore di posta certificata del mittente crea un nuovo messaggio, detto busta di trasporto, che contiene il messaggio originale e i principali dati di spedizione; la busta di trasporto viene firmata dal provider e per garantirne l'integrità del messaggio, mittente e destinatario sono costretti a utilizzare la casella PEC solo tramite protocolli sicuri.

Bisogna però operare una distinzione tra casi per quel che riguarda la comunicazione via PEC, ovvero il caso in cui si invia un messaggio tra due caselle PEC, quando un messaggio viene inviato da una casella PEC a una non PEC e quando il messaggio viene mandato da una casella non PEC a una PEC.

Nell'invio di un messaggio tra due caselle di posta PEC si procede come segue: il mittente invia una mail PEC, la quale verrà controllata dal proprio gestore per quanto riguarda la correttezza del messaggio e l'esistenza del de-

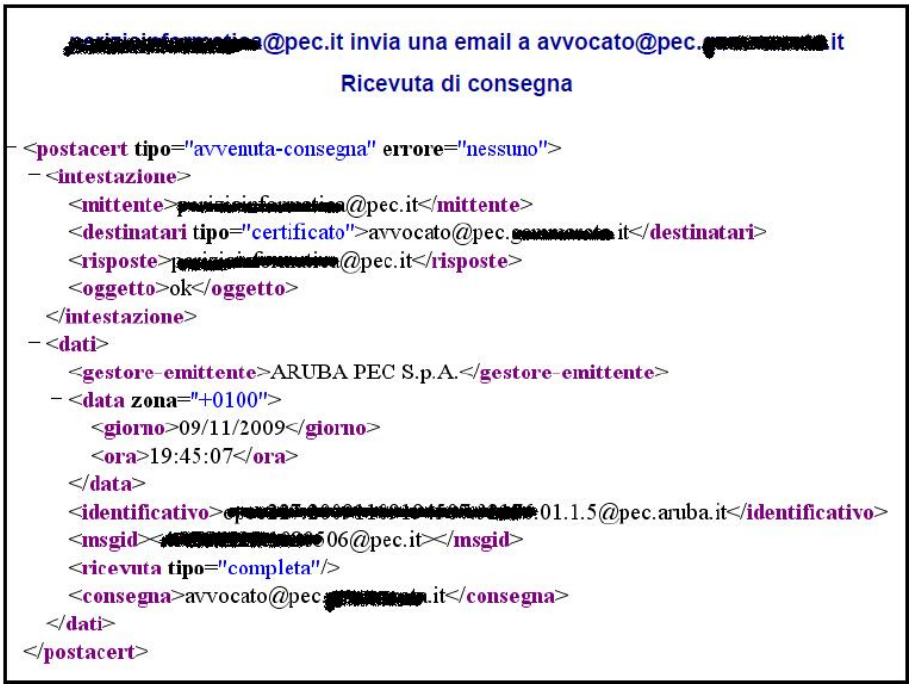

Figura 1.3: Ricevuta di consegna in una comunicazione via PEC

stinatario. Il gestore inoltre firmerà il messaggio che si desidera inviare, lo imbusterà e lo invierà all'altro gestore; il gestore del destinatario invece appena ricevuto il messaggio, invia la ricevuta di accettazione, successivamente invece invia la ricevuta di presa in carico e la ricevuta di consegna vera e propria. In ultimo quando l'utente destinatario accede alla casella di posta certificata, riceve il messaggio PEC in un' apposita busta firmata dal gestore del mittente.

Passiamo ora al caso di invio di messaggi tra una casella PEC e una non PEC: la trasmissione di messaggi tra PEC e non PEC è ammessa, ma non rappresenta un messaggio di posta elettronica certificata.

A differenza delle comunicazioni tra due PEC, in questa circostanza vi è solo un avviso nella ricevuta di accettazione della presenza di destinatari di posta ordinaria; inoltre non vi è nessuna ricevuta di consegna e i log registrano solo la prima parte di trasmissione.

In ultimo analizziamo il caso di invio di messaggi tra una casella non PEC e una PEC: anche in questo caso la trasmissione è consentita, ma anche qui non ci troviamo dinanzi a un invio di un messaggio di posta elettronica certificata; rispetto all'invio tra PEC e PEC manca la certificazione sulla provenienza del messaggio, ovvero non si hanno notizie sull'autenticità del mittente, ne sulla data e l'ora di invio e nemmeno sull'integrità del messaggio. In questa situazione il gestore del destinatario segnala la mancanza di certificazione inserendo il messaggio in una "busta anomala", evitando l'emissione di ricevuta di consegna.

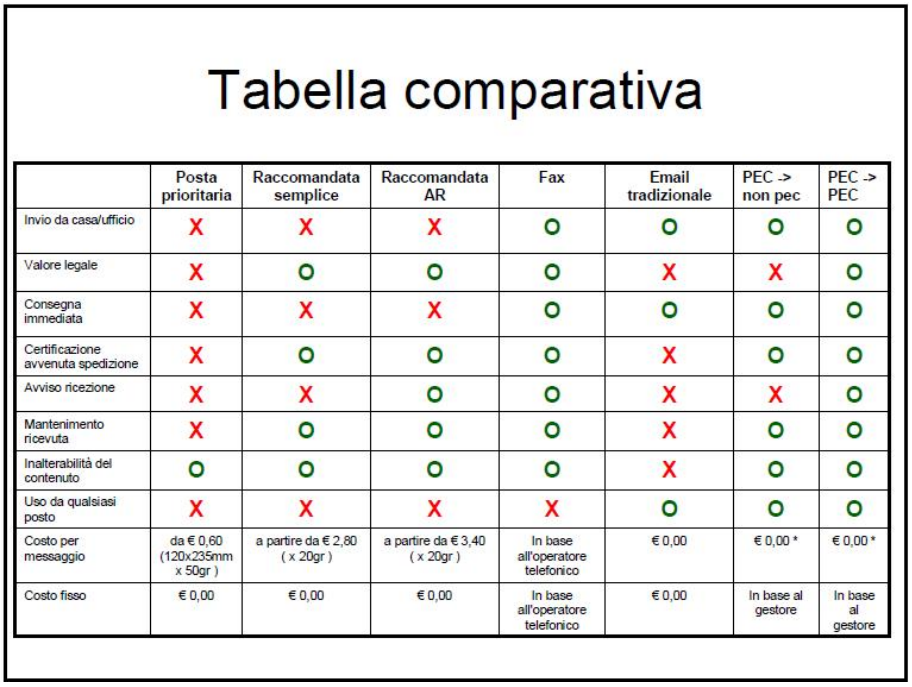

Tabella comparativa

	Posta prioritaria	Raccomandata semplice	Raccomandata AR	Fax	Email tradizionale	PEC -> non pec	PEC -> PEC
Invio da casa/ufficio	X	X	X	O	O	O	O
Valore legale	X	O	O	O	X	X	O
Consegna immediata	X	X	X	O	O	O	O
Certificazione avvenuta spedizione	X	O	O	O	X	O	O
Avviso ricezione	X	X	O	O	X	X	O
Mantenimento ricevuta	X	O	O	O	X	O	O
Inalterabilità del contenuto	O	O	O	O	X	O	O
Uso da qualsiasi posto	X	X	X	X	O	O	O
Costo per messaggio	da € 0,60 (120x235mm x 50gr)	a partire da € 2,80 (x 20gr)	a partire da € 3,40 (x 20gr)	In base all'operatore telefonico	€ 0,00	€ 0,00 *	€ 0,00 *
Costo fisso	€ 0,00	€ 0,00	€ 0,00	In base all'operatore telefonico	€ 0,00	In base al gestore	In base al gestore

Figura 1.4: Tabella comparativa dei principali mezzi per l'invio di messaggi

Si necessita di operare una distinzione tra le tipologie di ricevute "positive" in ambito di posta elettronica certificata. Sono tre le ricevute ai fini della certificazione del messaggio di PEC:

- di accettazione: attesta l'avvenuto invio della mail dal gestore di posta elettronica certificata al mittente

- di presa in carico: attesta il passaggio di responsabilità tra due distinti gestori di posta certificata. Questa ricevuta viene spesso scambiata tra i due gestori e non viene percepita dagli utilizzatori del servizio

- di avvenuta consegna: attesta che il messaggio è giunto a buon fine e che il destinatario ne ha piena disponibilità (anche se non ha ancora visto il messaggio).

Sono tre invece i tipi di avvisi rilanciati dal sistema PEC dopo il riscontro di problemi di comunicazione:

- di non accettazione: si rilevano utilizzi di mittente falso, destinatari in copia nascosta, vietati dalla PEC o altri problemi

- di mancata consegna: si riceve entro 12 ore, con avviso al mittente entro le successive 12 ore

- di rilevazione di virus informatici.

In caso di smarrimento di una delle ricevute presenti nel sistema PEC, è possibile disporre, presso i gestori del servizio, di una traccia informatica avente lo stesso valore legale in termini di invio o ricezione. Infine per quel che riguarda i gestori, va aggiunto che questi devono essere a termini di legge accreditati presso il CNIPA, che è l'organo pubblico preposto al controllo della posta elettronica certificata, e devono inoltre garantire l'uso di domini di posta dedicati (@postecert, @pec.it, @legamail.it....). Ogni gestore, nel rispetto della norma, deve sottoporsi ad una serie di test di interoperabilità, espressamente individuati sul sito del CNIPA. Questi ultimi devono essere effettuati per verificare la correttezza tecnico/funzionale del servizio di PEC erogato dal gestore.

Per una approfondimento specifico sul funzionamento della PEC riporto una parte interessante del documento "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata" (da www.digitpa.gov.it) :[urlb]

6 ELABORAZIONE DEI MESSAGGI

6.1 Formato dei messaggi generati dal sistema

Il sistema di PEC genera i messaggi (ricevute, avvisi e buste) in formato MIME. I messaggi sono composti da una parte di testo descrittivo, per l'utente, e da una serie di allegati (messaggio originale, dati di certificazione, ecc.) variabili a seconda della tipologia del messaggio.

Il messaggio (composto dall'insieme delle parti descritte nelle specifiche sezioni del presente allegato) è quindi inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del gestore di posta certificata. Il certificato associato alla chiave usata per la firma deve essere incluso in tale struttura. Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il "multipart/signed" (formato .p7s).

I messaggi sono trasferiti tra gestori usando una codifica a 7 bit sia per gli header sia per il corpo del messaggio e gli eventuali allegati. Per garantire la possibilità di verifica delle firme presenti sui messaggi di posta certificata, sul più ampio numero di client di posta elettronica possibile, i certificati X.509v3 utilizzati dai sistemi di posta elettronica certificata dovranno rispettare un determinato profilo.

Per garantire la verificabilità della firma da parte del client di posta ricevente, il mittente del messaggio deve coincidere con quello specificato all'interno del certificato usato per la firma S/MIME. Questo meccanismo comporta che le buste di trasporto riportino nel campo "From" un indirizzo di posta mittente differente da quello del messaggio originale. Al fine di consentire una migliore fruibilità del messaggio da parte dell'utente finale, l'indirizzo di posta mittente del messaggio originale è inserito come "display name" mittente nel messaggio. Ad esempio, per un messaggio originale con il seguente campo "From":

From: "Mario Bianchi" (*mario.bianchi@dominio.it*)

la relativa busta di trasporto generata avrà un campo "From" del tipo:

From: "Per conto di: mario.bianchi@dominio.it" ($posta{-}certificata@gestore.it$)

Per consentire che eventuali risposte alla busta di trasporto siano corret-

tamente indirizzate verso il mittente originale, è necessario che l'indirizzo di quest'ultimo sia riportato nel campo "Reply-To" della busta di trasporto. Qualora tale campo non fosse esplicitamente specificato nel messaggio originale, il sistema che genera la busta di trasporto provvede a crearlo estraendolo dal campo "From" del messaggio originale.

Per l'invio delle ricevute, il sistema usa come destinatario esclusivamente il mittente del messaggio originale così come specificato nel dato di "reverse path" del protocollo SMTP. Le ricevute devono essere inviate alla casella di posta certificata del mittente senza tenere conto del campo "Reply-To" eventualmente presente nell'intestazione del messaggio.

Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header specifico.

Ai fini della determinazione dei dati di certificazione fanno fede, per il sistema, gli elementi utilizzati per l'effettivo instradamento del messaggio verso i destinatari. Nelle fasi di colloquio mediante protocollo SMTP (ad esempio presso i punti di accesso e di ricezione) i dati di "reverse path" e "forward path" (comandi "MAIL FROM" e "RCPT TO") sono quindi considerati come dati di certificazione rispettivamente del mittente e dei destinatari. I dati di indirizzamento presenti nel corpo del messaggio (campi "To" e "Cc") sono usati esclusivamente per discriminare tra destinatari primari del messaggio e riceventi in copia, qualora necessario; i dati di indirizzamento presenti nel campo "Ccn" non sono considerati validi dal sistema.

6.2 Log

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema deve mantenere traccia delle operazioni svolte. Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:

- il codice identificativo univoco assegnato al messaggio originale (Message-ID)

- la data e l'ora dell'evento

- il mittente del messaggio originale
- i destinatari del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.)
- il gestore mittente

Gli effettivi dati registrati sui singoli log dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.). Deve essere garantita la possibilità di reperire, a richiesta, le informazioni contenute nei log.

6.3 Punto di accesso

Il punto di accesso consente ad un utente di accedere ai servizi di posta certificata resi disponibili dal proprio gestore. La possibilità da parte di un utente di accedere ai servizi di PEC deve prevedere necessariamente l'autenticazione dello stesso da parte al sistema (cfr. 8.3). Alla ricezione di un messaggio originale, il punto di accesso:

- effettua dei controlli formali sul messaggio in ingresso;
- genera una ricevuta di accettazione;
- imbusta il messaggio originale in una busta di trasporto.

La ricevuta di accettazione indica al mittente che il suo messaggio è stato accettato dal sistema e certifica la data e l'ora dell'evento. All'interno della ricevuta è presente un testo leggibile dall'utente, un allegato XML con i dati di certificazione in formato elaborabile ed eventuali altri allegati per funzionalità aggiuntive offerte dal gestore. Il punto di accesso, utilizzando i dati

dell'indice dei gestori di posta certificata (cfr. 7.5), effettua un controllo per ogni destinatario del messaggio originale per verificare se appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet). Tale controllo è realizzato verificando l'esistenza (mediante una ricerca "case insensitive") dei domini dei destinatari tra gli attributi "managedDomains" presenti all'interno dell'indice dei gestori. La ricevuta di accettazione (ed i relativi dati di certificazione) riporta quindi la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi (utenti di posta certificata, utenti esterni).

Deve essere garantita l'univocità dell'identificativo dei messaggi originali accettati nel complesso dell'infrastruttura di posta certificata per consentire una corretta tracciatura dei messaggi e delle relative ricevute. Il formato di tale identificativo è del tipo:

$(stringaalfanumerica)@(dominio - di - posta - gestore)$

oppure:

$(stringaalfanumerica)@(FQDN - server - di - posta)$

Il messaggio originale e la corrispondente busta di trasporto dovranno quindi contenere il seguente campo di header:

Message-ID: $(identificativomessaggio)$

Qualora il client di posta elettronica che colloquia con il punto di accesso avesse già inserito un Message ID all'interno del messaggio originale da inviare, questo dovrà essere sostituito con l'identificativo sopra descritto. Al fine di consentire al mittente l'associazione tra il messaggio inviato e le corrispondenti ricevute, l'eventuale Message ID originariamente presente nel messaggio dovrà essere inserito nel messaggio originale e nelle relative ricevute, avvisi e busta di trasporto. Se presente, il Message ID originale dovrà essere reso disponibile nell'intestazione del messaggio mediante l'inserimento del seguente header:

X-Riferimento-Message-ID: $(Message - IDoriginale)$

che sarà poi incluso all'interno delle ricevute e della busta di trasporto e riportato nei dati di certificazione (cfr. 7.4).

6.3.1 Controlli formali sui messaggi in ingresso

Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale verificando che:

- nel corpo del messaggio esista un campo "From" riportante un indirizzo email conforme alle specifiche RFC 2822 §3.4.1;
- nel corpo del messaggio esista un campo "To" riportante uno o più indirizzi email conformi alle specifiche RFC 2822 §3.4.1;
- l'indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato nel campo "From" del messaggio;
- gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) coincidano con quelli presenti nei campi "To" o "Cc" del messaggio;
- non siano presenti indirizzi dei destinatari del messaggio specificati nel campo "Ccn" del messaggio.

Qualora il messaggio non superi i controlli, il punto di accesso non dovrà accettare il messaggio all'interno del sistema di posta certificata emettendo il relativo avviso di non accettazione.

6.3.2 Avviso di non accettazione per eccezioni formali

Qualora il punto di accesso non possa provvedere all'inoltro del messaggio, a causa del mancato superamento dei controlli formali, viene recapitato al mittente uno specifico avviso di non accettazione.

Per questo avviso di non accettazione gli header contengono i seguenti campi:

X-Ricevuta: non-accettazione

Date: (*datadiemissionericevuta*)

Subject: AVVISO DI NON ACCETTAZIONE: (*subjectoriginale*)

From: posta-certificata@($dominio_di_posta$)

To: (*mittenteoriginale*)

X-Riferimento-Message-ID: ($Message - IDmessaggiooriginale$)

Il corpo del messaggio di questa ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

Errore nell'accettazione del messaggio

Il giorno (*data*) alle ore (*oraezona*)

nel messaggio ("*subject*")

proveniente da ("*mittenteoriginale*")

ed indirizzato a:

*destinatario*1

*destinatario*2

è stato rilevato un problema che ne impedisce l'accettazione

a causa di (*descrizioneerrore*).

Il messaggio non è stato accettato.

Identificativo messaggio: ($identificativo$)

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6 .3.3 Ricevuta di accettazione

La ricevuta di accettazione è costituita da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.

Negli header della ricevuta di accettazione sono inseriti i seguenti campi:

X-Ricevuta: accettazione

Date: ($effettivadatadiaccettazione$)

Subject: ACCETTAZIONE: ($subjectoriginale$)

From: posta-certificata@($dominio - di - posta$)

To: (*mittenteoriginale*)

X-Riferimento-Message-ID: ($Message - IDmessaggiooriginale$)

Il corpo del messaggio della ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporta i seguenti dati:

Ricevuta di accettazione

Il giorno (*data*) alle ore(*ora*) (*zona*)

il messaggio ("*subject*)"

proveniente da ("*mittenteoriginale*)"

ed indirizzato a:

(*destinatario*1) ("*postacertificata*) ("*postaordinaria*") (*destinatario*2) ("*postacertificata*") (" *postaordinaria*") .

.

.

(*destinatario*) ("*postacertificata*") ("*postaordinaria*")

è stato accettato dal sistema ed inoltrato.

Identificativo messaggio: (*identificativo*)

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

6.3.4 Busta di trasporto

La busta di trasporto consiste in un messaggio generato dal punto di accesso e che contiene il messaggio originale ed i dati di certificazione. La busta di trasporto eredita dal messaggio originale i seguenti header che dovranno quindi essere riportati immodificati:

- Received
- To
- Cc
- Return-Path

- Message-ID (così come descritto al punto 6.3) X-Riferimento-Message-ID (cfr. 6.3) X-TipoRicevuta

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

X-Trasporto: posta-certificata

Date: $(effettivadatadiaccettazione)$

Subject: POSTA CERTIFICATA: $(subjectoriginale)$

From: "Per conto di: $(mittenteoriginale)$"$(posta-certificata@dominio-di-posta)$)

Reply-To: (mittente originale $(inseritosoloseassente)$)

Il corpo della busta di trasporto è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio di posta certificata secondo un modello che riporti i seguenti dati di certificazione:

Messaggio di posta certificata

Il giorno $(data)$ alle ore (ora) $(zona)$) il messaggio

"$(subject)$" è stato inviato da "$(mittenteoriginale)$"

indirizzato a:

$(destinatario1)$

$(destinatario2)$

.

.

.

$(destinatario)$

Il messaggio originale è incluso in allegato.

Identificativo messaggio: $(identificativo)$

All'interno della busta di trasporto è inserito in allegato l'intero messaggio originale immodificato in formato conforme alla RFC 2822 (tranne per quanto detto a proposito del Message ID) completo di header, corpo ed eventuali allegati. Nella stessa busta di trasporto è inoltre incluso un allegato XML che specifica in formato elaborabile i dati di certificazione già riportati nel testo ed informazioni aggiuntive sul tipo di messaggio e tipo di ricevuta richiesta (cfr.

7.4). Alla busta di trasporto possono inoltre essere allegati ulteriori elementi opzionali per specifiche funzionalità fornite dal gestore di posta certificata. Anche se il campo "From" della busta di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento della busta di trasporto (forward path e reverse path del messaggio) rimangono immutati rispetto agli stessi dati del messaggio originale.

6.3.5 Avviso di mancata consegna per superamento dei tempi massimi previsti

Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di effettuare la consegna del messaggio. Tale comunicazione è effettuata mediante un avviso di mancata consegna per superamento dei tempi massimi nel quale gli header contengono i seguenti campi:

X-Ricevuta: preavviso-errore-consegna

Date: ($datadiemissionericevuta$)

Subject: AVVISO DI MANCATA CONSEGNA PER SUP. TEMPO MASSIMO: ($subjectoriginale$)

From: posta-certificata@($dominio - di - posta$)

To: ($mittenteoriginale$)

X-Riferimento-Message-ID: ($Message - IDmessaggiooriginale$)

Il corpo del messaggio del primo avviso di mancata consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

Avviso di mancata consegna

Il giorno ($data$) alle ore (ora) ($zona$) il messaggio

"($subject$)" proveniente da "($mittenteoriginale$)"

e destinato all'utente "($destinatario$)"

non e stato consegnato nelle prime dodici ore dal suo invio. Non escludendo che questo possa avvenire in seguito, si ritiene utile considerare che l'invio

del messaggio potrebbe non andare a buon fine. Il sistema provvederà comunque ad inviare un ulteriore avviso di mancata consegna se nelle prossime dodici ore non vi sarà la conferma della ricezione da parte del destinatario.

Identificativo messaggio: ($identificativo$)

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 e non prima delle 22 ore successive all'invio.

Il corpo del messaggio di questo avviso di mancata consegna, ha gli stessi header del precedente avviso, ed è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

Avviso di mancata consegna

Il giorno ($data$) alle ore (ora) ($zona$) il messaggio

"($subject$)" proveniente da "($mittenteoriginale$)"

e destinato all'utente "($destinatario$)"

non e stato consegnato nelle ventiquattro ore successive al suo invio. Si ritiene che la spedizione debba considerarsi non andata a buon fine.

Identificativo messaggio: ($identificativo$)

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6.4 Punto di ricezione

Il punto di ricezione permette lo scambio di messaggi di posta certificata

tra diversi gestori di posta certificata. È inoltre il punto attraverso il quale messaggi di posta elettronica ordinaria possono essere inseriti nel circuito della posta certificata

Lo scambio di messaggi tra diversi gestori avviene tramite una transazione basata sul protocollo SMTP come definito dalla RFC 2821. Eventuali errori verificatisi nel colloquio SMTP possono essere gestiti mediante i meccanismi standard di notifica degli errori propri del protocollo SMTP come previsto dalle RFC 2821 e RFC 1891. Tale sistema è adottato anche per la gestione di errori transitori in fase di trasmissione SMTP per i quali risulti un superamento del limite temporale di giacenza. Al fine di garantire al mittente una segnalazione dell'errore, coerentemente con le modalità definite nel paragrafo 6.3.5, i sistemi che gestiscono il traffico di posta certificata devono adottare come limite di tempo per la giacenza del messaggio un valore pari a 24 ore.

Il punto di ricezione, a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:

- verifica la correttezza/natura del messaggio in ingresso;
- se il messaggio in ingresso è una busta di trasporto corretta ed integra:
- emette una ricevuta di presa in carico verso il gestore mittente (cfr. 6.4.1);
- inoltra la busta di trasporto verso il punto di consegna (cfr. 6.5);
- se il messaggio in ingresso è una ricevuta corretta ed integra o un avviso di posta certificata corretto ed integro:
- inoltra la ricevuta/avviso verso il punto di consegna;
- se il messaggio in ingresso non risponde ai requisiti per una busta di trasporto o per una ricevuta/avviso corretto ed integro, ma risulta proveniente da un gestore di posta certificata, quindi supera le verifiche

di esistenza, provenienza e validità della firma, il messaggio deve essere propagato verso il destinatario, quindi:

- imbusta il messaggio in arrivo in una busta di anomalia (cfr. 6.4.2);
- inoltra la busta di anomalia verso il punto di consegna.
- se il messaggio in ingresso non proviene da un sistema di posta certificata, quindi non supera le verifiche di esistenza, provenienza e validità della firma, viene considerato di posta ordinaria, quindi, se propagato verso il destinatario:
- imbusta il messaggio in arrivo in una busta di anomalia (cfr. 6.4.2);
- inoltra la busta di anomalia verso il punto di consegna.

La ricevuta di presa in carico è emessa dal gestore ricevente il messaggio, nei confronti del gestore mittente. Il suo fine è quello di consentire il tracciamento del messaggio nel passaggio tra un gestore ed un altro.

Al ricevimento di un messaggio presso il punto di ricezione, il sistema compie i seguenti controlli, per verificare che la busta di trasporto/ricevuta/avviso sia corretta/integra:

- Controllo dell'esistenza della firma il sistema verifica la presenza della struttura S/MIME di firma all'interno del messaggio in ingresso;
- Controllo che la firma sia stata emessa da un gestore di posta certificata il punto di ricezione estrae il certificato usato per la firma del messaggio in ingresso e ne verifica la presenza all'interno dell'indice dei gestori di posta certificata. Per facilitare il controllo, è possibile calcolare l'hash SHA1 del certificato estratto ed effettuare la ricerca case insensitive della sua rappresentazione esadecimale all'interno degli attributi providerCertificateHash presenti nell'indice. Questa operazione consente di individuare agevolmente il gestore mittente per un successivo e necessario controllo della coincidenza del certificato estratto con quello presente nel record del gestore;

- Controllo della validità della firma è verificata la correttezza della firma S/MIME del messaggio effettuando il ricalcolo degli algoritmi di firma,la verifica della CRL e la validità temporale del certificato. Nel caso di utilizzo di meccanismi di replica locale (cache) dei contenuti delle CRL, deve essere adottato un intervallo di aggiornamento tale da garantire l'attualità del dato, al fine di minimizzare il possibile ritardo tra pubblicazione della revoca da parte della CA ed il recepimento di questa variazione da parte del gestore;

- Correttezza formale il gestore effettua le verifiche sufficienti e necessarie a garantire gli aspetti di correttezza formale necessari per l'interoperabilità.

  Nel caso di messaggi di posta ordinaria in ingresso al sistema di posta certificata, il gestore deve effettuare un controllo sulla presenza di virus informatici al fine di impedire l'introduzione di messaggi di posta ordinaria potenzialmente pericolosi, nel circuito della posta certificata. Nel caso di presenza di virus informatici in un messaggio di posta ordinaria, questo potrà quindi essere scartato dal punto di ricezione prima dell'ingresso nel circuito della posta certificata, senza quindi un trattamento particolare dell'errore ma con una gestione conforme alle pratiche comunemente adottate per i messaggi sulla rete pubblica.

  Quando in fase di ricezione viene rilevata la presenza di un virus all'interno di una busta di trasporto, il gestore del destinatario emette un avviso di rilevazione virus informatico destinato al punto di consegna del gestore mittente.

  Il gestore mittente, alla ricezione di un avviso di rilevazione virus informatico, di cui al paragrafo 6.4.3, dovrà : 1. controllare periodicamente quali tipologie di virus non sono state rilevate dal proprio sistema antivirus al fine di comprenderne le motivazioni e verificare l'opportunità di eventuali interventi, 2. inviare gli eventuali avvisi di mancata consegna per virus, destinati al mittente del messaggio.

6.4.1 Ricevuta di presa in carico

Allo scambio di messaggi di posta certificata corretti tra differenti gestori di posta certificata, il gestore ricevente emette una ricevuta di presa in carico nei confronti del gestore mittente. Le ricevute di presa in carico emesse sono relative ai destinatari ai quali è indirizzato il messaggio in ingresso, così come specificato nei dati di instradamento (forward path e reverse path) della transazione SMTP. All'interno dei dati di certificazione della singola ricevuta di presa in carico sono elencati i destinatari a cui la stessa fa riferimento. In generale, a fronte di una busta di trasporto, ogni gestore destinatario dovrà emettere una o più ricevute di presa in carico per i destinatari di propria competenza. L'insieme di tali ricevute coprirà, in assenza di errori di trasporto, il complessivo dei destinatari del messaggio.

Gli header di una ricevuta di presa in carico contengono i seguenti campi:

X-Ricevuta: $presa - in - carico$

Date: ($datadipresaincarico$)

Subject: PRESA IN CARICO: ($subjectoriginale$)

From: posta-certificata@($dominio - di - posta$)

To: ($ricevutegestoremittente$)

X-Riferimento-Message-ID: ($Message - IDmessaggiooriginale$)

L'indirizzo per l'invio delle ricevute al gestore mittente è ricavato dall'indice dei gestori di posta certificata durante l'interrogazione necessaria per il controllo del soggetto che ha emesso la firma nella verifica del messaggio in ingresso.

Il corpo del messaggio di una ricevuta di presa in carico è composto secondo un modello riportante i seguenti dati:

Ricevuta di presa in carico

Il giorno ($data$) alle ore (ora) ($zona$)

il messaggio "($subject$)"

proveniente da "($mittente$)"

ed indirizzato a:

($destinatario1$)

(*destinatario*2) . . . (*destinatarion*)

è stato accettato dal sistema.

Identificativo messaggio: (*identificativo*)

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

6.4.2 Busta di anomalia

Nel caso in cui uno dei test evidenzi un errore nel messaggio in arrivo, oppure venga riconosciuto come un messaggio di posta ordinaria e il gestore preveda la propagazione verso il destinatario, il sistema lo inserisce in una busta di anomalia. Prima della consegna, il messaggio pervenuto al punto di ricezione completo di header , testo ed allegati è inserito in formato conforme alla RFC 2822 come allegato all'interno di un nuovo messaggio che eredita dal messaggio in arrivo i seguenti header che dovranno quindi essere riportati immodificati:

- Received
- To
- Cc
- Return-Path
- Message-ID

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

X-Trasporto: *errore*

Date: [*datadiarrivodelmessaggio*]

Subject: ANOMALIA MESSAGGIO: [*subjectoriginale*]

From: "Per conto di: [*mittenteoriginale*] (*posta−certificata*@(*dominio−di − posta*))

Reply-To: [*mittenteoriginale*(*inseritosoloseassente*)]

Il corpo della busta di anomalia è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio secondo un modello che riporti i seguenti dati:

Anomalia nel messaggio

Il giorno [*data*] alle ore [*ora*] [*zona*] è stato ricevuto

il messaggio "[*subject*]" proveniente da "[*mittenteoriginale*]"

ed indirizzato a:

[*destinatario*1] [*destinatario*2] . . . [*destinatarion*]

Tali dati non sono stati certificati per il seguente errore:

[*descrizionesinteticaerroreriscontrato*]

Il messaggio originale è incluso in allegato.

Nella busta di anomalia non sono inseriti allegati oltre al messaggio pervenuto al punto di ricezione (es. dati di certificazione) data l'incertezza sull'effettiva provenienza/correttezza del messaggio.

Anche se il campo "From" della busta di anomalia è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento della busta di anomalia (forward path e reverse path del messaggio) rimangono immutati rispetto agli stessi dati del messaggio originale. In questo modo è garantito sia l'inoltro del messaggio verso i destinatari originari sia il ritorno di eventuali notifiche di errore sul protocollo SMTP (come da RFC 2821 e RFC 1891) al mittente del messaggio.

6.4.3 Avvisi relativi alla rilevazione di virus informatici 6.4.3.1 Avviso di non accettazione per virus informatico

Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione.

Il punto di accesso deve compiere dei controlli sul contenuto del messaggio in ingresso e non accettarlo qualora all'interno di questo o di uno dei suoi eventuali allegati, fosse identificata la presenza di virus informatici. In questo caso deve essere emesso l'avviso di non accettazione per virus informatico per

dare chiara comunicazione al mittente dei motivi che hanno portato al rifiuto del messaggio.

Per questo avviso di non accettazione gli header contengono i seguenti campi:

X-Ricevuta: $non - accettazione$

X-VerificaSicurezza: $errore$

Date: [$datadiemissionericevuta$]

Subject: AVVISO DI NON ACCETTAZIONE PER VIRUS: [$subjectoriginale$]

From: posta-certificata@[$dominio - di - posta$]

To: [$mittenteoriginale$]

X-Riferimento-Message-ID: [$Message - IDmessaggiooriginale$]

Il corpo del messaggio di questa ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

Errore nell'accettazione del messaggio per presenza di virus

Il giorno [$data$] alle ore [ora] [$zona$]

nel messaggio "[$subject$]"

proveniente da "[$mittenteoriginale$]"

ed indirizzato a: [$destinatario1$] [$destinatario2$]

è stato rilevato un problema di sicurezza [$identificativodeltipodicontenutorilevato$].

Il messaggio non è stato accettato.

Identificativo messaggio: [$identificativo$]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6.4.3.2Avviso di rilevazione virus informatico

Qualora il gestore del destinatario riceva messaggi di posta elettronica certificata con virus informatici è tenuto a non inoltrarli, informando tempe-

stivamente il gestore del mittente affinchè comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione.

Nel caso nella fase di ricezione si evidenzi la presenza di virus informatici nel messaggio di posta elettronica certificata la cui provenienza sia stata accertata dalle verifiche effettuate sulla firma del gestore mittente, il sistema genera un avviso di rilevazione virus da restituire al gestore mittente indicando come indirizzo quello specificato per le ricevute nell'Indice dei gestori di posta certificata, con l'indicazione dell'errore riscontrato.

Per questo avviso di rilevazione virus gli header contengono i seguenti campi:

X-Ricevuta: $rilevazione - virus$

X-Mittente: [$mittenteoriginale$]

Date: [$datadiemissionericevuta$]

Subject: PROBLEMA DI SICUREZZA: [$subjectoriginale$]

From: posta-certificata@[$dominio - di - posta$]

To: [$ricevutegestoremittente$]

X-Riferimento-Message-ID: [$Message - IDmessaggiooriginale$]

Il corpo del messaggio di questo avviso è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

Avviso di rilevazione virus informatico

Il giorno [$data$] alle ore [ora] [$zona$] nel messaggio

"[$subject$]" proveniente da "[$mittenteoriginale$]"

e destinato all'utente "[$destinatario$]"

è stato rilevato un problema di sicurezza [$identificativodeltipodicontenutorilevato$].

Identificativo messaggio: [$identificativo$]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso, per permetterne un'elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

Nel corpo del messaggio deve essere specificato il motivo per il quale è stato impossibile dar corso alla trasmissione.

6.4..3.3Avviso di mancata consegna per virus informatico

All'arrivo di un avviso di rilevazione di virus informatico proveniente dal gestore destinatario, il gestore del mittente emette un avviso di mancata consegna da restituire al mittente.

Per questo avviso di mancata consegna gli header contengono i seguenti campi:

X-Ricevuta: $errore - consegna$

X-VerificaSicurezza: $errore$

Date: [$datadiemissionericevuta$]

Subject: AVVISO DI MANCATA CONSEGNA PER VIRUS: [$subjectoriginale$]

From: posta-certificata@[$dominio - di - posta$]

To: [$mittenteoriginale$]

X-Riferimento-Message-ID: [$Message - IDmessaggiooriginale$]

Il corpo del messaggio di questo avviso di mancata consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

Avviso di mancata consegna per virus

Il giorno [$data$] alle ore [ora] [$zona$]

nel messaggio "[$subject$]"

destinato all'utente "[$destinatario$]"

è stato rilevato un problema di sicurezza [$identificativo - del - tipo - di - contenuto - rilevato$].

Il messaggio non è stato consegnato.

Identificativo messaggio: [$identificativo$]

Tutte le informazioni necessarie per la costruzione di questo avviso derivano da quanto contenuto nel correlato avviso di rilevazione virus.

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4).

All'interno dell'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

Nel corpo del messaggio deve essere specificato il motivo per il quale è stato impossibile dar corso alla trasmissione.

6.5 Punto di consegna

6.5.1 Verifiche sui messaggi in ingresso

All'arrivo del messaggio presso il punto di consegna, il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta al mittente. La ricevuta di avvenuta consegna è emessa dopo che il messaggio è stato consegnato nella casella di posta del destinatario ed esclusivamente a fronte della ricezione di una busta di trasporto valida, identificabile dalla presenza dell'header: X-Trasporto: posta-certificata

In tutti gli altri casi (es. buste di anomalia, ricevute), la ricevuta di avvenuta consegna non è emessa. In ogni caso, il messaggio ricevuto dal punto di consegna deve essere consegnato immodificato alla casella di posta del destinatario.

La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente ed un allegato XML con i dati di certificazione, oltre ad eventuali allegati per funzionalità aggiuntive offerte dal gestore.

Se il messaggio pervenuto al punto di consegna non fosse recapitabile alla casella di destinazione, il punto di consegna emette un avviso di mancata consegna (cfr. 6.5.3). L'avviso di mancata consegna è generato, a fronte di un errore, relativo alla consegna di una busta di trasporto corretta.

6.5.2 Ricevuta di avvenuta consegna

6.5.2.1 Ricevuta completa di avvenuta consegna

Le ricevute di avvenuta consegna sono costituite da un messaggio di posta elettronica inviato al mittente che riporta la data e l'ora di avvenuta consegna, i dati del mittente e del destinatario e l'oggetto.

Negli header delle ricevute di avvenuta consegna sono inseriti i seguenti

campi:

X-Ricevuta: $avvenuta - consegna$

Date: [$datadiconsegna$]

Subject: CONSEGNA: [$subject - originale$]

From: posta-certificata@[$dominio - di - posta$]

To: [$mittente - originale$]

X-Riferimento-Message-ID: [$Message - IDmessaggio - originale$]

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

Ricevuta di avvenuta consegna

Il giorno [$data$] alle ore [ora] [$zona$]

il messaggio "[$subject$]"

proveniente da "[$mittenteoriginale$]"

ed indirizzato a "[$destinatario$]"

è stato consegnato nella casella di destinazione.

Identificativo messaggio: [$identificativo$]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Nel rilascio delle ricevute di avvenuta consegna, il sistema distingue tra i messaggi consegnati ai destinatari primari ed i riceventi in copia. Tale verifica è effettuata mediante l'analisi dei campi "To" (destinatari primari) e "Cc" (riceventi in copia) del messaggio rispetto al destinatario oggetto della consegna. Esclusivamente per le consegne relative ai destinatari primari, all'interno della ricevuta di avvenuta consegna, oltre agli allegati descritti, è inserito il messaggio originale completo (header, testo ed eventuali allegati). Il sistema deve adottare una logica cautelativa nella valutazione della tipologia destinatario (primario o ricevente in copia) e nella conseguente decisione di

non inserire il messaggio originale nella ricevuta di avvenuta consegna. Qualora il sistema che effettua la consegna non potesse determinare con certezza la natura del destinatario (primario od in copia) per problemi di ambiguità dei campi "To" e "Cc", la consegna dovrà essere considerata come indirizzata ad un destinatario primario ed includere il messaggio originale completo.

6.5.2.2 Ricevuta di avvenuta consegna breve

Al fine di consentire uno snellimento dei flussi, è possibile, per il mittente, richiedere la ricevuta di avvenuta consegna in formato breve. La ricevuta di avvenuta consegna breve inserisce al suo interno il messaggio originale, sostituendone gli allegati con i relativi hash crittografici per ridurre le dimensioni della ricevuta. Per permettere la verifica dei contenuti trasmessi è indispensabile che il mittente conservi gli originali immodificati degli allegati inseriti nel messaggio originale, a cui gli hash fanno riferimento.

Se all'interno della busta di trasporto è presente l'intestazione:

X-TipoRicevuta: *breve*

il punto di consegna emette, per i destinatari primari, una ricevuta di avvenuta consegna breve. L'assenza di tale intestazione o un valore diverso da 'breve' o 'sintetica' (cfr 6.5.2.3) comportano l'elaborazione della ricevuta di avvenuta consegna secondo le modalità già descritte al punto 6.5.2.1. Il valore dell'intestazione nella busta di trasporto deriva dal messaggio originale (cfr. 6.3.4) permettendo così al mittente di stabilire il formato delle ricevute di avvenuta consegna relative ai destinatari primari del messaggio originale. Per i destinatari riceventi in copia, le ricevute di avvenuta consegna seguono quanto descritto al punto 6.5.2.

Negli header delle ricevute brevi di avvenuta consegna sono inseriti i seguenti campi:

X-Ricevuta: $avvenuta - consegna$

Date: $[data - di - consegna]$

Subject: CONSEGNA: $[subject - originale]$

From: posta-certificata@$[dominio - di - posta]$

To: $[mittente - originale]$

X-Riferimento-Message-ID: [$Message - IDmessaggio - originale$]

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

Ricevuta breve di avvenuta consegna :
Il giorno [*data*] alle ore [*ora*] [*zona*]
il messaggio "[*subject*]"
proveniente da "[*mittenteoriginale*]"
ed indirizzato a "[*destinatario*]"
è stato consegnato nella casella di destinazione.
Identificativo messaggio: [$identificativo$]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Alla ricevuta breve di avvenuta consegna è allegato il messaggio originale nel quale rimane inalterata la struttura MIME, ma i cui allegati sono sostituiti da altrettanti file di testo contenenti gli hash del file al quale si vanno a sostituire. Gli allegati sono identificati dalla presenza del parametro "name" nell'intestazione "content-type" oppure "filename" nell'intestazione "content-disposition" della parte MIME.

Nel caso di messaggi originali in formato S/MIME è necessario non alterare l'integrità della struttura del messaggio modificando le parti MIME proprie della costruzione S/MIME. La verifica della natura S/MIME del messaggio originale avviene controllando il MIME type dell'entità di livello più alto (coincidente con il messaggio stesso). Un messaggio S/MIME può avere i seguenti MIME type (come da RFC 2633):

- multipart/signed

Il MIME type rappresenta un messaggio originale firmato dal mittente secondo la struttura descritta dalla RFC 1847. Il messaggio è formato da

due parti MIME: la prima che costituisce il messaggio composto dal mittente prima della sua firma e la seconda che contiene i dati di firma. La seconda parte (generalmente di tipo application/pkcs7-signature oppure - application/x-pkcs7-signature) contiene i dati aggiunti durante la fase di firma del messaggio e deve essere lasciata inalterata per non compromettere la struttura complessiva del messaggio;

- application/pkcs7-mime oppure application/x-pkcs7-mime

Questi MIME type sono generalmente associati a messaggi crittografati, anche se in alcune particolari implementazioni possono rappresentare messaggi firmati od altri oggetti crittografici. Il messaggio è composto da un unico oggetto CMS contenuto all'interno della parte MIME. Data l'impossibilità di distinguere gli allegati eventualmente presenti all'interno dell'oggetto CMS, la parte MIME viene lasciata intatta senza essere sostituita dal relativo hash, di fatto determinando l'emissione di una ricevuta di avvenuta consegna breve con gli stessi contenuti di una normale ricevuta di avvenuta consegna.

L'individuazione delle parti da non sottoporre alla sostituzione con i corrispondenti hash deve basarsi sul MIME type del messaggio (entità MIME di livello più alto) e sull'eventuale sottostruttura MIME interna. I MIME type delle parti di livello inferiore così come i nomi dei file delle parti stesse non devono essere usati come elementi discriminanti per evitare ambiguità con allegati utente aventi stessi tipi od estensioni. Nel caso il messaggio originale contenga allegati il cui Content-Type risulti message/rfc822, ossia contenga un messaggio di posta come allegato, l'intero messaggio allegato viene sostituito con il relativo hash.

In generale, nel caso di messaggi originali in formato S/MIME, la copia del messaggio contenuta all'interno della ricevuta di avvenuta consegna breve avrà le seguenti caratteristiche:

- se il messaggio originale è firmato, la struttura S/MIME ed i relativi dati di firma resteranno inalterati. Il messaggio genererà un errore in un'eventuale fase di verifica dell'integrità della firma, in seguito alla sostituzione degli allegati con i relativi hash;

- se nel messaggio originale è presente il MIME Type :application/pkcs7-mime oppure application/x-pkcs7-mime : gli allegati contenuti nel messaggio non saranno sostituiti dagli hash data l'impossibilità di identificarli all'interno del blocco crittografico. Il contenuto della ricevuta di avvenuta consegna breve coinciderà quindi con quello di una normale ricevuta di avvenuta consegna. L'algoritmo utilizzato per il calcolo dell'hash è il Secure Hash Algorithm 1 (SHA1), così come descritto dalla RFC 3174 calcolato sull'intero contenuto dell'allegato. Per consentire di distinguere i file contenenti gli hash dai file a cui fanno riferimento, il suffisso ".hash" è aggiunto al termine del nome originale del file. L'hash è scritto all'interno del file con rappresentazione esadecimale come un'unica sequenza di 40 caratteri. Il MIME type di questi allegati è impostato a "text/plain" per evidenziare la loro natura testuale.

6.5.2.3 Ricevuta sintetica di avvenuta consegna

Se all'interno della busta di trasporto è presente l'intestazione:

X-TipoRicevuta: *sintetica*

il punto di consegna emette, sia per i destinatari primari sia per i riceventi in copia, una ricevuta di avvenuta consegna sintetica.

Negli header delle ricevute sintetiche di avvenuta consegna sono inseriti i seguenti campi:

X-Ricevuta: $avvenuta - consegna$

Date: [$datadiconsegna$]

Subject: CONSEGNA: [$subjectoriginale$]

From: posta-certificata@[$dominio - di - posta$]

To: [$mittenteoriginale$]

X-Riferimento-Message-ID: [$Message - IDmessaggio - originale$]

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

Ricevuta sintetica di avvenuta consegna

Il giorno [$data$] alle ore [ora] [$zona$]

il messaggio "[*subject*]"

proveniente da "[*mittenteoriginale*]"

ed indirizzato a "[*destinatario*]"

è stato consegnato nella casella di destinazione.

Identificativo messaggio: [$identificativo$]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Il valore dell'intestazione nella busta di trasporto deriva dal messaggio originale (cfr. 6.3.4) permettendo così al mittente di stabilire il formato delle ricevute di avvenuta consegna relative ai destinatari primari del messaggio originale.

La ricevuta sintetica di avvenuta consegna segue le medesime regole di emissione della ricevuta di avventa consegna; in allegato non contiene il messaggio originale ma contiene esclusivamente il file XML contenente i dati di certificazione descritti nella ricevuta di avvenuta consegna.

6.5.3Avviso di mancata consegna

Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera un avviso di mancata consegna da restituire al mittente con l'indicazione dell'errore riscontrato.

Per un avviso di mancata consegna gli header contengono i seguenti campi:

X-Ricevuta: $errore - consegna$

Date: [$data - di - emissione - ricevuta$]

Subject: AVVISO DI MANCATA CONSEGNA: [*subjectoriginale*]

From: posta-certificata@[$dominio - di - posta$]

To: [*mittenteoriginale*]

X-Riferimento-Message-ID: [$Message - IDmessaggio - originale$]

Il corpo del messaggio di un avviso di mancata consegna è composto da

un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

Avviso di mancata consegna
Il giorno [*data*] alle ore [*ora*] [*zona*]
nel messaggio "[*subject*]"
proveniente da "[*mittenteoriginale*]"
e destinato all'utente "[*destinatario*]"
è stato rilevato un errore [*erroresintetico*].
Il messaggio è stato rifiutato dal sistema.
Identificativo messaggio: [*identificativo*]

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne un'elaborazione automatica (cfr. 7.4). All'interno dell'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

Dopo aver analizzato lo strumento atto a prevenire violazioni della privacy nello scambio di dati e nelle comunicazioni, spostiamo l'attenzione su come si riesce a firmare un documento informatico, in modo da renderlo paragonabile, agli effetti legali, alle sottoscrizioni tradizionali cartacee.

Analizzeremo dunque tutti gli aspetti legati alle firme digitali e alle firme elettroniche, dandone inizialmente una definizione esaustiva, considerando gli aspetti tecnici e le metodologie di funzionamento, e spostando poi l'attenzione sugli enti certificatori che con essa lavorano.

Capitolo 2

Firma Digitale e Firma Elettronica

2.1 Firma Digitale e Firma Elettronica

Con l'espressione firma elettronica (electronic signature) si intende qualunque metodo e tecnologia attraverso cui si può firmare un documento informatico[1].[Zag00]

Nella più ampia categoria delle firme elettroniche, possiamo distinguere le firme elettroniche "sicure" o "avanzate", definite tali in quanto in possesso di requisiti e funzionalità che offrono garanzie tali da poterle paragonare, agli effetti legali, alle sottoscrizioni cartacee tradizionali.

La firma elettronica avanzata viene definita dalla direttiva CE come "una firma elettronica che soddisfi i seguenti requisiti:

- essere connessa in maniera unica al firmatario
- essere idonea ad identificare il firmatario
- essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo

[1]Zagami R., Firma digitale e sicurezza giuridca, CEDAM

- essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati".

La direttiva CE non menziona mai l'espressione "firma digitale", tuttavia, è evidente che il concetto di firma elettronica avanzata è stato formulato tenendo in considerazione le caratteristiche delle firme digitali e della certificazione delle chiavi.[Mai02]

Il limite principale delle firme elettroniche non sicure o non avanzate sta nel fatto che non hanno alcun legame con il documento dove sono apposte, potendo essere duplicate e riutilizzate.

Queste definizioni di firma elettronica, analogamente a quelle poste da altri provvedimenti internazionali, adottano un approccio aperto, non presupponendo il necessario impiego di una determinata tecnologia, ma lasciando in teoria il campo aperto a tutti quei sistemi che realizzano, comunque, i requisiti e le funzioni indicati. Peraltro, questa apertura di principio non si è ancora concretizzata nell'indicazione di ben individuati sistemi, differenti dalla cifratura asimmetrica.

La firma digitale, come delineata dalla normativa italiana, è un tipo di firma elettronica sicura, basata sulla cifratura asimmetrica e su una infrastruttura di certificazione.

Firma digitale e firma elettronica non sono sinonimi nella terminologia usata dal legislatore italiano.

"Firma elettronica" designa un genere e "firma digitale" una specie[2].[Fin]

La firma digitale apposta o associata ad un documento informatico, equivale alla sottoscrizione tradizionale prevista per gli atti e i documenti in forma scritta su supporto cartaceo. Essa è il risultato di una procedura informatica (validation) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consentono al sottoscrittore, tramite chiave privata, e al destinatario, tramite 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.

[2]Finocchiaro G., Diritto di Internet, Zanichelli Bologna

La sua funzione principale è quella di conferire al documento informatico, inteso in senso lato, i fondamentali requisiti di integrità, paternità, riservatezza e non ripudio. L'apposizione della stessa, inoltre, integra e sostituisce l'apposizione di sigilli, punizioni, timbri, contrassegni e marchi di qualsiasi genere.

Il termine crittografia deriva dalla parola greca *kriptos*, ovvero nascosto, e *graphia*, che significa scrittura. Codificare o cifrare dei dati significa trasformarli in una forma non leggibile da coloro i quali non dispongono della cosiddetta chiave di cifratura. L'idea della codifica delle informazioni risale ad almeno quattromila anni fa, quando gli Egiziani usavano geroglifici modificati per incidere i propri messaggi funerari. Tale operazione, tuttavia, veniva utilizzata non tanto per rendere segreto il messaggio, quanto per la preziosità estetica[3].[Gia00]

Le tecniche di cifratura elaborate e sviluppate per proteggere i documenti informatici durante la fase di trasmissione attraverso reti telematiche si sono rivelate un supporto necessario alla teorizzazione della validità giuridica dei documenti formati attraverso un elaboratore elettronico, ed inoltre l'unica possibile e percorribile via attraverso la quale si è giunti a definire il documento elettronico e la sua entrata a tutti gli effetti nel *corpus* normativo del nostro ordinamento giuridico.

La definizione di firma digitale, cosi come contemplata dall'art. 1, d.p.r. 513/97, rimane sempre valida, nonostante la sovrapposizione di successivi contributi normativi sia nazionali che sovranazionali, in quanto i requisiti previsti dal nostro legislatore ai fini della sua validità coincidono con quelli del legislatore comunitario ove definisce la tipologia della "firma elettronica avanzata".

Fondamentalmente la firma digitale è un informazione che viene aggiunta al documento redatto per mezzo di un elaboratore elettronico al fine di garantirne integrità e provenienza.

[3]Giannaccari A., La crittografia come strumento per garantire la riservatezza delle comunicazioni, Rivista Diritto Informatico, 2000

La crittografia si basa essenzialmente sull'applicazione, al testo da cifrare, di una funzione matematica (c.d. Algoritmo di codifica) azionabile mediante un apposito codice (c.d. Chiave). L'algoritmo di codifica è una funzione reversibile: ne deriva che l'applicazione a contrario dello stesso algoritmo e della chiave, permette di rendere di nuovo leggibile il testo originario.

L' algoritmo più utilizzato in ambito di crittografia simmetrica è il Data Encryption Standard (DES), che ha visto la luce grazie ad alcuni ricercatori IBM e che successivamente è stato adottato come standard delle agenzie federali degli Stati Uniti verso la metà degli anni settanta. L'algoritmo di codifica più utilizzato in ambito di crittografia asimmetrica è invece l'R.S.A(riconosciuto dal nostro legislatore come standard, unitamente all'algoritmo DSA: cfr. art.2 del D.P.C.M. 8 febbraio 1999). Prende il nome dalle iniziali dei cognomi dei suoi autori(Rivest, Shamir, Adleman), ricercatori del M.I.I, che lo svilupparono nel 1977[4].[Rog99]

Le tecniche di crittografia sono suddivisibili principalmente in due categorie:

- crittografia simmetrica, o a chiave privata: si basa sull'utilizzazione di un unica chiave sia per cifrare che per decifrare il testo

- crittografia asimmetrica, o a chiave pubblica: si basa sull'utilizzazione di una coppia di chiavi (una privata, l'altra pubblica) fra di loro in una relazione biunivoca[5]; una viene utilizzata per cifrare il testo, l'altra per decifrarlo.

In altri termini, il documento codificato con una delle due chiavi può essere decodificato solo con l'altra chiave, e non riutilizzando la prima (c.d. Complementarità delle chiavi).

La scelta del legislatore italiano è caduta sulla seconda delle categorie

[4]G.Rognetta, la firma digitale e il documento informatico, Napoli 1999

[5]Biunivocità è termine che indica la corrispondenza secondo cui ad ogni elemento di un insieme corrisponde uno ed un solo dell'altro e viceversa, cioè per ogni chiave privata è impossibile aversi due chiavi pubbliche identiche e viceversa

sopra menzionate[6], perchè l'utilizzatore di un sistema di crittografia simmetrica non avrebbe soddisfatto quel principio di certezza de diritto che doveva (e deve) caratterizzare le operazioni negoziali del commercio virtuale, al pari delle operazioni contrattuali concluse mediante strumenti tradizionali.

In particolare, per quanto riguarda l'ambito contrattuale (e specificatamente il momento perfezionativo), un sistema di crittografia simmetrica si rivela idoneo a tutelare, al più, l'esigenza di riservatezza dei dati; inidoneo, invece, a tutelare la non contraffazione dei medesimi (integrità), a dimostrare la provenienza delle informazioni (autenticità), nonché a garantire la non ripudiabilità (chi trasmette/riceve non può negare di aver trasmesso/ricevuto).

Infatti, l'utilizzazione di un unica chiave tanto per cifrare quanto per decifrare il testo, può esporre a questo pericolo: in fase di formazione di un accordo contrattuale, X, accettante, dopo aver decifrato con l'apposita chiave il messaggio contenente la proposta di Y, la modifichi a suo piacimento prima dell'accettazione e sostenga poi la provenienza da Y. È ovvio che questa si configurerebbe come una soluzione inammissibile sul piano della certezza del diritto.

A ciò si aggiunga che dovrebbero generarsi tante chiavi quante potrebbero essere le coppie contrattuali (proponente/accettante) potenziali utilizzatrici del sistema, e che, in difetto di un canale sicuro di trasmissione della chiave (e tale non può essere considerata, senza ulteriori accorgimenti tecnici, la rete telematica), si paleserebbe la necessità di un incontro fisico fra le due parti per concordare il codice comune. Eventualità, quest'ultima, di certo non in linea con un sistema che dovrebbe funzionare anche tra interlocutori separati da grandi distanze.

[6]Con tutti i correttivi del caso: ci si riferisce al sistema di certificazione "verticale" delle chiavi pubbliche, affidato ad apposite società di certificazione (in possesso di particolari requisiti relativamente alla loro struttura e alle modalità di esercizio della loro attività: cfr., rispettivamente, articoli 8-9 del D.P.R. 513/97 e il D.P.C.M. 8 febbraio 1999), in luogo di quello "orizzontale" utilizzato diffusamente in internet da parte degli utenti del software Pretty Good Privacy

A questi inconvenienti sopperisce un sistema di crittografia (o sistema di validazione, secondo la definizione datane dall'art.1, lett. c) del D.P.R. 513/97), a chiavi asimmetriche, perché le firme digitali contribuiscono a tutelare la riservatezza, l'integrità, l'autenticità, nonché a garantire (attraverso un apposito sistema di certificazione delle c.d. Public keys) la non ripudiabilità dei contenuti di un documento informatico[7].

Infatti, a differenza del sistema tradizionale simmetrico, il sistema a chiavi asimmetriche consta di due chiavi di cifratura attribuite a ogni utilizzatore: denominate "privata" l'una, in uso esclusivo del soggetto titolare, e "pubblica", quella destinata a essere pubblicata negli appositi registri on-line (c.d. *Keysrepositories*), accessibili a chiunque.

Si può ora passare a prendete in considerazione le possibili applicazioni della crittografia a chiave pubblica, non senza però ribadire le condizioni essenziali per il corretto funzionamento (anche giuridico) del sistema:

- la chiave privata deve essere conosciuta solo dal soggetto titolare di essa (art. 1, lett. e del D.P.R. 513/97)[8]

- la conoscenza della chiave pubblica non deve permettere di risalire alla chiave privata (c.d. Indipendenza delle chiavi), in esclusiva disponibilità, quest'ultima, del soggetto titolare.

[7]Non si può ovviamente ottenere la certezza matematica, valida semper et semper, della c.d. Inviolabilità di un sistema informatico. In riferimento a chiavi asimmetriche del tipo adottato dal nostro legislatore (in base all'algoritmo RSA la lunghezza delle chiavi può essere di 384, 512 o 1024 bit), è stato calcolato che "una rete di un milione di computer impiegherebbe un tempo corrispondente all'età dell'universo per ricavare una chiave privata da una chiave pubblica. Questo non esclude che in futuro si possa violare ciò che oggi appare inviolabile: ciò che conta, però, è che, allo stato delle attuali conoscenze tecniche, il sistema sia completamente affidabile". G. Rognetta, la firma digitale e il documento informatico

[8]E, secondo quando disposto dall art. 9, primo comma, del D.P.R. 513/97, deve rimanere nella sua esclusiva disponibilità, di modo che un uso illegittimo della chiave configurerebbe un caso di responsabilità oggettiva per danno a terzi nel caso che il titolare non "adotti tutte le misure organizzative e tecniche idonee ad evitare danno ad altri"

La funzione di segretezza del documento è assicurata cifrando il testo in oggetto con la chiave pubblica del destinatario. Il destinatario userà la propria chiave privata (corrispondente a quella pubblica utilizzata dal mittente) per decifrarlo. È importante notare che, data la biunivocità delle chiavi, solo il destinatario, e nessun altro, potrà cifrare il documento (fig. 5).

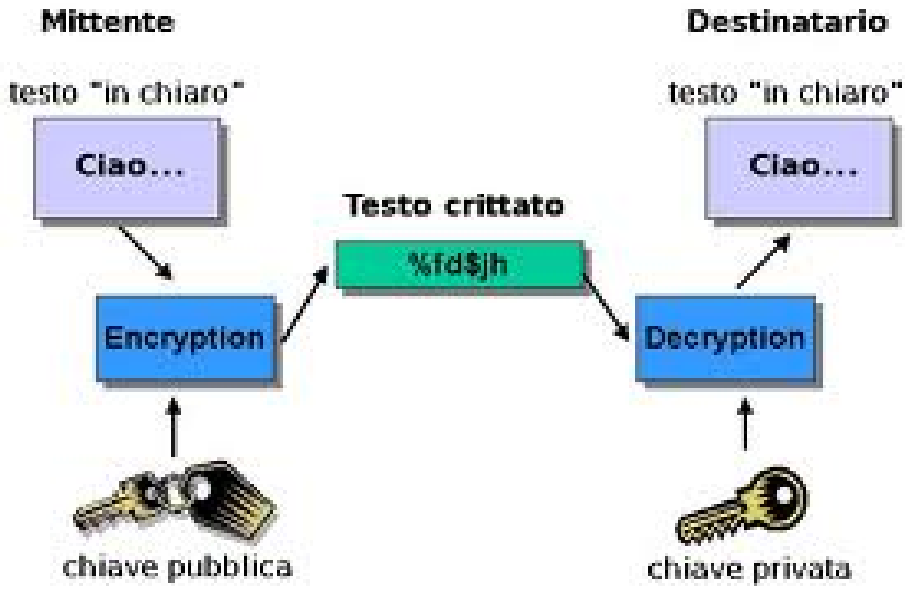

Figura 2.1: Tecnica di protezione della riservatezza attraversola crittografia a chiave pubblica

Tramite questa prima applicazione del sistema non viene però garantita ne l'integrità ne la provenienza del documento, perché chiunque potrebbe impossessarsi della chiave pubblica del destinatario e inviargli un documento cifrato, nel caso, una proposta contrattuale via mail, attribuendosi un falso nome o spendendo, illegittimamente, un nome altrui.

L'autenticità del documento e la sua integrità vengono assicurate mediante la seconda delle possibili applicazioni della crittografia asimmetrica, ed è in tale operazione che si genera la firma digitale. Infatti una "firma digitale è il risultato dell'applicazione di una chiave privata ad un documento informatico. Chiunque voglia verificare la sua autenticità applicherà la chiave

pubblica corrispondente e potrà essere certo, da un lato, della provenienza di un documento da parte di una persona che ha la disponibilità della chiave privata; dall'altro, dell'integrità dello stesso al momento dell'applicazione della firma digitale"[9]

La firma digitale può essere applicata tanto all'intero documento quanto ad un estratto di esso (il c.d. *Messagedigest* o *hashcode*, ottenuto tramite l'applicazione al documento informatico di una particolare funzione matematica, la c.d. Funzione di Hash). Il risultato (visivo) che si ottiene è il seguente: un insieme incomprensibile di caratteri alfanumerici sostitutivi dell'intero documento, nel primo caso; sostitutivi di una parte, solamente nel secondo.

Figura 2.2: La tecnica di autenticazione attraverso la crittografia a chiave pubblica

E' bene sottolineare che la modifica, anche di una sola piccola parte, del messaggio originale, dopo l'apposizione della firma digitale tramite la chiave privata, renderebbe negativa la verifica che il destinatario fa con la corrispondente chiave pubblica.

Se invece la verifica ha esito positivo, il destinatario acquista la certezza giuridica che il documento proviene da chi ha la disponibilità della chiave privata corrispondente, e che il documento non ha subito alterazioni.

[9]Da Zagami R., firma digitale

Riassumendo: con questa seconda applicazione si riscontrano gli aspetti positivi correlati all'uso della firma digitale, ovvero la pronta e semplice verifica della firma attraverso strumenti informatici, la rilevanza oggettiva della relativa indagine, la non contraffazione dei dati in mancanza della detenzione della chiave privata segreta, da un lato, il suo legame indissolubile con il documento, dall'altro.

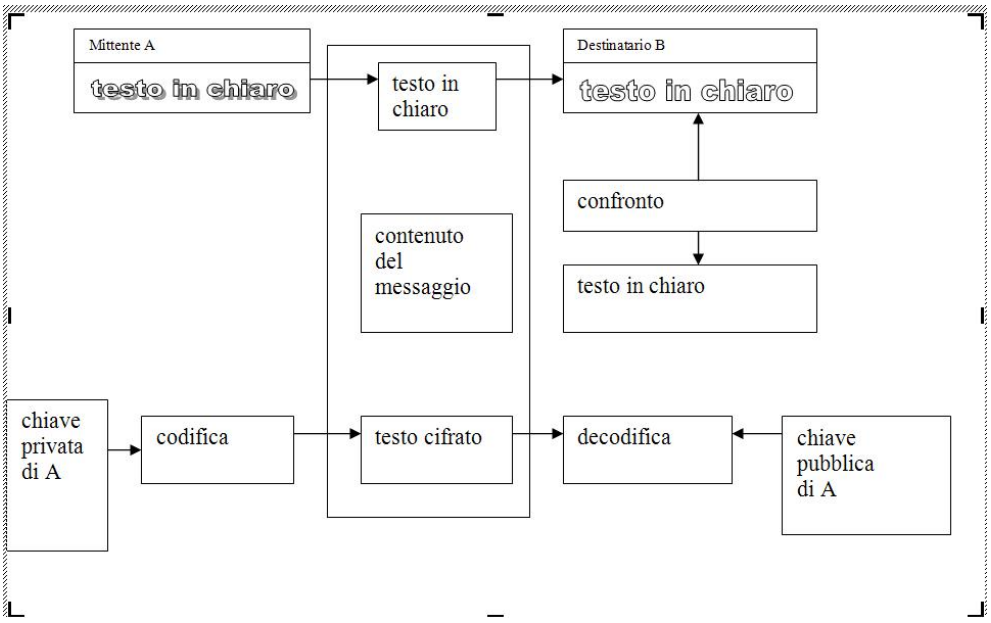

Figura 2.3: Lo schema di funzionamento della firma digitale

Di contro questa seconda applicazione non tutela la riservatezza, atteso che chiunque dispone del documento può leggerlo, applicando la chiave pubblica del sottoscrittore, prelevata on-line dal c.d. *Keyrepositories*. Combinando, però, le due applicazioni, sopra esemplificate, si riesce ad assicurare nel contempo, la riservatezza del contenuto dei dati, l'autenticità e l'integrità degli stessi (fig.8). Qualora, infatti, il mittente utilizzi la propria chiave privata per firmare digitalmente il documento e quella pubblica del destinatario per cifrarlo, quest'ultimo lo decifrerà utilizzando la propria chiave privata (ottenendo, terminata questa prima operazione, un testo ancora cifrato, essendo quest'ultimo il risultato dell'apposizione della firma digitale all'origine)

e ne verificherà l'autenticità e l'integrità, usando la chiave pubblica del mittente (ottenendo, terminata questa seconda operazione e se la verifica da esito positivo, un testo perfettamente leggibile e comprensibile).

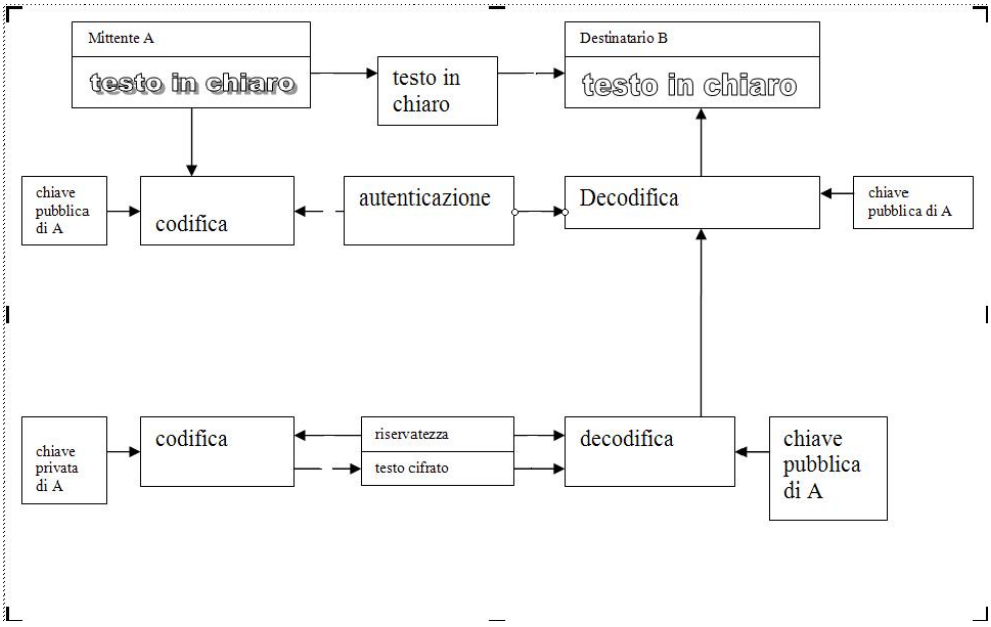

Figura 2.4: Autenticazione e riservatezza attraverso la crittografia a chiave pubblica

A conclusione di questa breve disamina su come funzioni il sistema di firma digitale, occorre un ulteriore precisazione: si è precedentemente constatato che, risultato dell'applicazione della firma digitale a un documento elettronico è, da un lato, la possibilità di verificare l'integrità del documento firmato e, dall'altro, la possibilità di accertamento della paternità dello stesso, nel senso che a verifica positiva corrisponde la certezza che quel documento è stato firmato dal titolare della chiave privata che ha generato quella firma.

In breve: viene in evidenza, nel sistema fin qui descritto, la mancanza di un indicazione certa circa la reale identità del titolare della coppia di chiavi; mancanza che potrebbe permettere a chiunque di creare delle coppie di chiavi, associarle ad un nome di un altra persona, pubblicare on-line la

chiave pubblica e quindi usare il nome falso e la chiave privata corrispondente per generare firme digitali.

Ci si troverebbe di fronte ad un problema di inattendibilità dell'attribuzione delle chiavi pubbliche, che non può permettersi, pena la perdita di ogni certezza giuridica[10].

Per questo il D.P.R. 513/97 all'art. 8 disciplina la figura dei certificatori: società per azioni, con un capitale sociale non inferiore a quello necessario per svolgere l'attività bancaria, in possesso di particolari requisiti gestionali, tecnici e organizzativi, la cui attività è monitorata costantemente dal CNIPA.

La funzione principale cui queste società sono deputate è, appunto, l'attività di certificazione definita all'articolo 1 lett. h), del D.P.R. 513/97 come "il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato(...)". Ad un accertamento ex post della provenienza oggettiva di un documento informatico, da intendersi come corrispondenza biunivoca fra un determinato documento informatico, non alterato successivamente la sua creazione, e la chiave privata utilizzata per firmarlo, si affianca, cosi, un accertamento ex ante della provenienza soggettiva di una determinata coppia di chiavi. Viene cosi garantita la piena equiparabilità, dal punto di vista funzionale, tra la sottoscrizione tradizionale e la firma digitale.

[10] È quello che succede in pratica con il diffusissimo programma di crittografia asimmetrica PGP, il quale si basa in sostanza su un attività di certificazione c.d. Orizzontale. Il PGP non prevede l'esistenza di un autorità di certificazione che garantisca la corrispondenza tra una coppia di chiavi e il suo titolare; il programma, infatti, consente ad ogni utente di firmare, con la propria chiave privata, la chiave pubblica di un altro utente, rendendola cosi valida. In sostanza, un utente funge da potenziale certificatore per gli altri utenti

2.2 Evoluzione dei principali aspetti normativi: dagli albori ai giorni nostri

Il nostro Paese è stato il primo in Europa a legiferare in materia di firma elettronica, o più esattamente di firma digitale, e a predisporre il corredo dei relativi regolamenti. Era il 1997: a breve distanza seguì la Germania, con un sistema legislativo simile a quello italiano, anche se originato in modo differente. Gli altri Paesi della Comunità si sono mossi dopo e solo a seguito di una specifica direttiva europea.

Inizialmente si è ricorsi a una serie di norme derivanti dalla legge sulla "Riforma della pubblica amministrazione e per la semplificazione amministrativa" n. 59 del 15 marzo 1997 [11], che all'articolo 15, comma 2, recita: "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, nonchè la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri e le modalità di applicazione del seguente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti....".

Questo articolo ha introdotto nell'ordinamento italiano il principio generale della validità e della rilevanza giuridica delle rappresentazioni informatiche.

La norma non era nata per disciplinare il commercio elettronico, e quindi per fini privatistici, ma per un esigenza delle pubbliche amministrazioni, quella di trasmettere atti giuridici in rete. Questa esigenza è emersa chiaramente con il progetto RUPA, ovvero Rete Unitaria della Pubblica Amministrazione, rete destinata a collegare tra loro le PA, istituito tramite DPCM del 5/09/1995. Si tratta di un progetto intersettoriale prioritario per il perseguimento degli obbiettivi di efficienza, miglioramento dei servizi, potenziamenti dei supporti conoscitivi e contenimento dei costi dell'azione amministrativa.

La rete era stata creata per poter offrire un sistema informativo inte-

[11] G.U. n.63 del 17 marzo 1997

grato permettendo alle singole amministrazioni, da un lato, di comunicare tra di loro per lo scambio di ogni documento ed informazione utile, dall'altro, di proporsi verso la collettività come centro unitario erogatore di dati e prestazioni amministrative favorendo, cosi, il rapporto del cittadino con l'Amministrazione e il decentramento effettivo di quest'ultima.

La rete unitaria, che si manifesta come un sistema integrato delle singole reti, quindi come "rete di reti", avrebbe dovuto condurre all'utilizzazione ottimale delle risorse telematiche e a significative economie nei costi di impianto e di esercizio[12].

Lo studio di fattibilità della rete[13] al paragrafo 7.3.5[14] [Fin03] dice:

"Affinché le amministrazioni possano avvalersi a tutti gli effetti di legge delle tecnologie informatiche e telematiche, occorre un'apposita previsione normativa che attribuisca piena rilevanza giuridica ai dati contenuti nei sistemi informativi e agli atti amministrativi emanati attraverso i sistemi medesimi. Tale rilevanza deve essere subordinata alla conformità dei dati e degli atti amministrativi e a regole tecniche definite da queste Autorità, finalizzate, in particolare, a garantire la sicurezza dei dati e la riservatezza della persona. L'opportunità di siffatto intervento di carattere normativo discende da talune incertezze interpretative sulle norme già esistenti in materia..."

Quindi prende espressamente in considerazione gli aspetti giuridici ed evidenzia la necessità di evitare interpretazioni che possano mettere in dubbio il valore giuridico del documento elettronico. L'eventualità di rendere obbligatoria una stampa cartacea del documento elettronico per conferire all'atto giuridico in esso contenuto piena rilevanza giuridica, avrebbe inevitabilmente compromesso il successo del progetto.

In ogni modo, le disposizioni della 1. 69 del 1997, se da un lato consacrano il ruolo del mezzo informatico come strumento di semplificazione amministrativa, di miglioramento dei servizi forniti dagli uffici pubblici e di

[12] Art 1-2 DPCM 05/09/1995

[13] Consultabile sul sito dell'AIPA

[14] Cfr. Finocchiaro G., firma digitale e firme elettroniche: profili privatistici Giuffrè, Milano 2003

razionalizzazione della spesa pubblica, dall'altro la formulazione generica ne estende il raggio di azione al di là del settore pubblico. La norma imponeva di fatto i medesimi criteri e modalità di applicazione sia per il settore pubblico che per quello privato, contrapponendosi ad una tradizione consolidata di rigorosa separazione tra i due ambiti[15].[Cev02]

Inoltre, possiamo notare che l'articolo 15 della 1. 59/97 menziona atti, dati, documenti e contratti, richiamando entità disomogenee sotto il profilo giuridico. Pure risultavano differenti gli stadi dell'atto, del dato, del documento e del contratto in cui la rappresentazione informatica viene in rilievo.

Poi con il decreto del Presidente della Repubblica n. 513 del 10 novembre 1997[16] fu emanato il "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione dei documenti con strumenti informatici e telematici". Questo individuò le modalità concrete di attuazione del principio generale sancito dalla legge precedentemente trattata e stabilì cosi i criteri di equivalenza fra documento informatico e documento scritto. In tal modo, si è avuto l'introduzione della firma digitale nel sistema giuridico italiano.

La tecnica normativa inizialmente scelta dal legislatore italiano, in parte modificata dopo l'attuazione della direttiva comunitaria, consisteva nell'affermazione del principio generale della validità e della rilevanza giuridica delle rappresentazioni informatiche e nell'equiparazione dei documenti informatici, a seconda delle caratteristiche presentate, a fattispecie diverse già disciplinate dal codice civile.

Inoltre, venne fissata l'equivalenza tra il documento informatico e quello scritto e fra la sottoscrizione autografa e la firma digitale, anche se con limitazione e precisazioni.

Il DPR 513 all'articolo 3, comma 1, prescrive che con il decreto del Presidente del Consiglio dei ministri siano "fissate le regole tecniche per la for-

[15]Cfr. Cevenini C., il documento informatico e la firma digitale, in Pattaro E.(a cura di), manuale di diritto dell'informatica e delle nuove tecnologie, CLUEB, Bologna 2002

[16]G.U. n.60 del 13 marzo 1998

mazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici". Questo DPCM venne emanato l'8 febbraio del 1999[17]:è un documento tecnicamente molto dettagliato, che si differenziava con particolare attenzione sulle problematiche di sicurezza informatica. Tra l'altro, fissò le regole in base alle quali un ente poteva essere iscritto, a sua domanda, nell'elenco pubblico dei certificatori e assegna all'Autorità per l'informatica nella pubblica amministrazione (Aipa)[18] i compiti di approvare l'inserimento nell'elenco di un nuovo certificatore e di tener aggiornato l'elenco stesso. A questo riguardo, l'Aipa, in data 26 luglio 1999, ha emesso la circolare n.22[19] che ha stabilito le modalità con le quali vanno presentate le domande da parte dei candidati certificatori.

In riferimento alla questione dell'interoperabilità, poiché le norme del DPCM unite alle regole tecniche non bastavano a garantirla, l'Aipa, in data 19 giugno 200, ha emesso la circolare n.24[20] che ha fissato le "linee guida per l'interoperabilità dei certificatori iscritti nell'elenco pubblico".

L'interoperabilità della firma digitale è alla base del processo di diffusione ed utilizzo di questa. Consiste nel fatto che un certificato emessa da una determinata CA, possa essere validato e letto da un utente che si avvale dei servizi di una diversa CA.

Altra fondamentale circolare Aipa è la numero 27 del 16 febbraio 2001[21] che disciplinò l'utilizzo della firma digitale nell'ambito della PA.

Poi il 28 dicembre 2000, con il DPR 513/97 n. 445[22] è stato emanato il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, che incorporava le norme del DPR 513/97 sulla firma digitale, che pertanto venne abrogato.

Le disposizioni del DPR 513/97 confluirono sostanzialmente , anche se con modifiche, nel DPR 445/2000. Comunque, la modifica più rilevante fù

[17] G.U n, 87 del 15 aprile 1999
[18] Attualmente CNIPA, istituito con il D.legisl. N. 196/2003
[19] G.U. n. 179 del 2 agosto 1999
[20] G.U. n. 151 del 30 giugno 2000
[21] G.U. n. 47 del 26 febbraio 2001
[22] G.U. n. 42 del 20 febbraio 2001

quella concernente l'efficacia probatoria della firma digitale, disciplinata prima dall'articolo 5 del decreto 1997 e poi dall'articolo 10 del decreto 2000. L'articolo 5 non risultava molto chiaro; infatti disponeva: "il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 cod. civ.", ma alcun requisito era indicato nel regolamento eccetto quello della firma digitale.

Inoltre non poteva interpretarsi come diretta a regolare il documento informatico munito di firma digitale, dal momento che quest'ultima era già regolata dal primo comma del medesimo articolo 5 che sosteneva: "il documento informatico sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'art. 2702 del cod. civ.".

Ne consegue che l'interpretazione preferita pareva essere quella secondo la quale il primo comma dell'articolo 5 disciplinava il documento informatico senza firma digitale.

L'articolo 10 del Testo Unico sulla documentazione amministrativa ha riformulato tale articolo, anche se non contribuendo a chiarire.

Esso disponeva al primo comma: "il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui all'articolo 8, 2° comma e per le pubbliche amministrazioni, anche di quelle cui all'articolo 9, 4° comma, soddisfa il requisito legale della forma scritta e ha l'efficacia probatoria ai sensi dell'articolo 2712 del codice civile".

Invece il comma 3 del medesimo articolo disponeva: "il documento informatico sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile". In tal modo, al documento informatico con firma digitale veniva attribuita sia l'efficacia probatoria delle riproduzioni meccaniche, sia l'efficacia probatoria della scrittura privata.

I pochi commentatori che avevano affrontato l'argomento avevano cercato di attribuire un significato diverso ai termini "documento informatico" e "firma digitale", a seconda che i suddetti termini fossero contenuti nel primo comma dell'articolo 10 del Testo Unico, pur ricorrendo la medesima espres-

sione "documento informatico sottoscritto con firma digitale", e nel terzo comma.

C'è chi aveva proposto di attribuire al documento informatico un significato diverso a seconda che si trattasse di testo o di documento informatico contenente suoni e immagini[23].

Ma la definizione normativa di firma digitale, all'articolo 1 del T.U. 445/2000 modificata dal DPR 137/2003, pareva non lasciare spazio ad ambiguità; la firma digitale veniva definita come "il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

Poi, all'inizio del 2000, venne pubblicata la direttiva europea n. 93/1999, relativa a un quadro unitario delle firme elettroniche, ma il dibattito avvenuto durante la preparazione durò almeno due anni, con uno scontro tra la visione giuridica continentale, più rigorosa, di quella anglosassone, più permissiva.

Il fatto che la funzione considerata preminente sia stato quello della comunicazione, ha permesso che prevalessero le considerazioni più legate alla categoria della libertà delle comunicazioni.

La direttiva si componeva delle seguenti parti:

- un preambolo con ventotto "considerando"
- un insieme di norme distribuite in quindici articoli, di cui i primi dieci meno importanti
- quattro allegati

I ventotto "considerando" danno la dimensione della pluralità dei punti di vista e delle conseguenti soluzioni di compromesso.

[23]Cfr. Finocchiaro G., Firma digitale e firme elettroniche: profili privatistici, GIUFFRE' editore, Milano 2003

Vengono enunciati dei "principi", genericamente esposti, e la direttiva prescinde volutamente da considerazioni di tipo tecnologico, per cui il contenuto delle norme risultava spesso troppo generico e di difficile interpretazione.

Non vi è traccia dell'impostazione normativa italiana, molto particolareggiata e attenta agli aspetti tecnici, caratterizzata da un unico tipo di firma e di certificatore, da un altissimo grado di sicurezza e da una diffusa concretezza. Invece, lo spirito prevalente nella direttiva era quello del libero commercio e della libera iniziativa in un mercato aperto, in base alla quale, ad esempio, si danno poteri amplissimi a certe categorie di certificatori senza sottoporli a nessuna forma di controllo preventivo.

Il fatto che la direttiva mostrò di essere poco dettagliata tecnicamente, la spinse a trattare in maniera approssimativa problemi fondamentali come quelli dell'interoperabilità. Cosi, erroneamente, la direttiva europea emanata sembrava ignorare le problematiche tecniche che si possono manifestare in materia di comunicazione fra utenti e interoperabilità fra certificatori.

È evidente che, nella stesura della direttiva, la presenza italiana non risultò significativa.

Il T.U. n.445/2000 all'articolo 8, comma 2, stabiliva: "Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definiti con decreto del Presidente del Consiglio dei ministri o, per sua delega, del Ministro per l'innovazione e la tecnologia, sentito il Ministero per la funzione pubblica e il Garante per la protezione dei dati personali. Esse sono adeguate alle esigenze dettate dalla soluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno biennale".

Le regole tecniche hanno lo scopo di dare ai certificatori delle guide precise anche di tipo organizzativo, a garanzia del perfetto funzionamento del servizio che viene loro affidato. Il criterio prevalente era quello della sicurezza che doveva risultare costantemente al più elevato livello possibile.

Una prima versione delle regole fu emanata con il DPCM 8 febbraio 1999; una seconda versione, che abroga la prima, con un DPCM pubblicato nel

2003. Le due versioni differivano in pochi punti, in base all'esperienza e a qualche esigenza dovuta al recepimento della direttiva europea.

L'articolo 3 del DPR 513/1997 prima e poi l'articolo 8 del DPR 445/2000, a loro volta, rinviavano la definizione di alcuni rilevanti aspetti della disciplina del documento informatico e della firma digitale a regole tecniche. Queste riguardavano la formazione, la trasmissione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, nonché le misure tecniche, organizzative e gestionali, volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche.

Una parte significativa delle questioni tecniche sarà disciplinata dal DPCM 8 febbraio 1999, "Regole per la formazione, la trasmissione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513". Il decreto si componeva di tre articoli e di un corposo allegato tecnico di 63 articoli.

Nel frattempo era stata emanata la direttiva europea n.93 del 13 dicembre 1999[24] relativa a un "Quadro comunitario per le firme elettroniche".

Il sistema introdotto dal legislatore italiano nel 1997 traeva la sua motivazione dalla legge sulla semplificazione amministrativa e aveva lo scopo di dare valore legale ai documenti informatici sottoscritti digitalmente.

Al contrario, la direttiva europea ignorava del tutto l'esperienza italiana e si ispirò al commercio elettronico e ai concetti di liberalizzazione.

Questi diversi punti di vista crearono non pochi problemi di coerenza e compatibilità nella costruzione del sistema italiano. Anche la successiva dicitura voluta dalla direttiva europea (firma elettronica anziché firma digitale) non facilitò la chiarezza.

Con la "Legge comunitaria 2000" n. 422 del 29 dicembre 2000[25], il Parlamento delegò il Governo a recepire la direttiva europea, avvenuto con il

[24] G.U.CE. L 13 del 13 gennaio 2000
[25] G.U. n.14 del 20 gennaio 2001

decreto legislativo n. 10 del 23 gennaio 2002[26] , "Attuazione della direttiva 1993/93 CE relativa a un quadro comunitario per le firme elettroniche".

Quest'ultimo decreto ha profondamente modificato il quadro normativo previgente, disciplinando, oltre alla firma digitale, le firme elettroniche.

L'articolo 13 del decreto prevedeva modifiche alla normativa, disponendo: "entro trenta giorni dalla data di entrata in vigore del presente decreto è emanato un regolamento , ai sensi dell'articolo 17, 2° comma, della L. 23 agosto 1988, n. 400, anche ai fini del coordinamento delle disposizioni del testo unico emanato con il decreto del Presidente della Repubblica 28 dicembre 2000, n.445, con quelle recate dal presente decreto e dalla Direttiva 1999/93/CE, nonché dalla fissazione dei requisiti necessari per lo svolgimento dell'attività dei certificatori."

Il panorama si presentava cosi caratterizzato da una sorta di "doppio binario": la firma digitale, da un lato, le firme elettroniche, a loro volta distinte -secondo il recente DPR 137/2003- in firme elettroniche, firme elettroniche avanzate e firme elettroniche qualificate, dall'altro. A questi "diversi binari" il legislatore associò un diverso valore giuridico e una diversa efficacia probatoria.

Inoltre, con il DPCM del 30/10/2003, si introdusse anche lo "Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione" che, tra l'altro, individuò l'organismo pubblico incaricato di accreditare i centri di valutazione e di certificare le valutazioni di sicurezza. Il decreto prevedeva che con apposito DPR, si adottava un regolamento per coordinare le disposizioni del T.U. con quelle recate dal decreto legislativo stesso.

Il regolamento, che è stato emanato con il DPR 7 aprile 2003, n.137[27] , andava a sua volta a modificare il suddetto T.U.

Aveva un duplice scopo:

- coordinare le disposizioni del DPR 445/2000 sulla firma digitale e le

[26] G.U, n.29 del 15 febbraio 2002
[27] G.U. n.138 del 17 giugno 2003

disposizioni del Decreto Legislativo del 2002 sulle firme elettroniche

- stabilire i nuovi requisiti per lo svolgimento dell'attività dei certificatori

Il decreto coordinava le due normative di origine diversa e di oggetto diverso: quella del DPR 445/2000, tutta italiana, sulla firma digitale, e quella del Decreto Legislativo n.10 del 2002, di derivazione europea, sulle firme elettroniche.

Il decreto 137/2003 coordinava differenti tipologie di firme: in particolare, vennero definite quattro tipi di firme , la firma digitale, la firma elettronica qualificata, la firma elettronica avanzata e la firma elettronica.

Inoltre stabilì i requisiti dei certificatori "qualificati" e "accreditati", le cui figure furono introdotte dal Decreto Legislativo 10/2002.

Poi, con il DPCM n.98 del 27/04/2004 furono anche emanate delle nuove regole tecniche che sostituirono quelle del DPCM 8 febbraio 1999.

2.3 Certificatori

In materia di firme, un ruolo di grande importanza è rivestito dal certificatore, detto anche Autorità di certificazione o in lingua inglese CA, Certification Authority.

È necessario premettere che i termini "certificatore", "certificato" e "certificazione" vengono utilizzati dal legislatore con un significato prettamente tecnico e connesso con il sistema di firme elettroniche e di firma digitale.

Il certificatore è stato definito, dall'articolo 2, 1° comma, lett. b) del Decreto Legislativo 10/2002, come "il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime".

I certificati elettronici, allo stesso comma, lett. d) sono gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi.

Quindi la funzione fondamentale del certificato è di consentire l'attribuzione della firma elettronica al titolare del dispositivo di firma o dei dati uti-

lizzati per verificare la firma, al fine di confermare l'identità. Il certificatore è chi presta questo servizio.

Secondo l'attuale normativa si hanno 2 tipi di certificato:

- certificato elettronico (art.2, comma 1, lett. d) del D.Lgs. 23 gennaio 2002, n.10)
- certificato qualificato (art.2, comma 1, lett. e) del D.Lgs. 23 gennaio 2002, n.10 e articolo 27/bis del DPR 445/2000, come modificato dal DPR 137/2003)

Mentre sono tre i tipi di certificatore:

- certificatore (art. 4 del D.Lgs. 10/2002 e art. 26 del DPR 445/2000, come modificato dal DPR 137/2003)
- certificatore qualificato (art. 4 del D.Lgs. 10/2002 e art. 27 del DPR 445/2000 come modificato dal DPR 137/2003)
- certificatore accreditato (art.5 del D.Lgs. 10/2002 e art. 28 del DPR 445/2000, come modificato dal DPR 137/2003)

Il sistema precedentemente adottato (con il DPR 513/1997 e, poi, con il DPR 445/2000) era molto differente: c'era un solo tipo di certificato e un unico certificatore. I compiti di quest'ultimo erano strettamente collegati alla tecnologia adoperata, cioè alla certificazione della chiave pubblica, collegata alla chiave privata. Si considerava certificatore, il soggetto pubblico o privato che effettuava la certificazione, rilasciava il certificato della chiave pubblica, lo pubblicava insieme ad essa, pubblicava e aggiornava gli elenchi dei certificati sospesi e revocati, gestiva gli elenchi delle chiavi pubbliche. La sua funzione principale era di garantire la corrispondenza tra un soggetto e la sua chiave pubblica mediante la certificazione (art. 28-bis e 29-bis del DPR 445/2000 come modificato dal DPR 137/2003).

Occorre mettere in evidenza che il meccanismo di firma elettronica non consente di identificare il soggetto che di fatto appone la firma, ma il soggetto

titolare della chiave, del dispositivo o dei dati con i quali la firma viene apposta. Per rendere più stretto il collegamento tra queste due figure è possibile ricorrere a chiavi biometriche, sistemi di identificazione e autorizzazione basati su caratteristiche fisiche, personalissime se non esclusive, di un soggetto, quali le impronte digitali o l'impronta della retina.

La direttiva n. 93 del 1999, il Decreto Legislativo 10/2002 di attuazione della direttiva e il DPR 137/2003 hanno modificato la normativa sui certificatori.

La disciplina fu successivamente dettata dagli articoli 26-29- quinquies del DPR 445/2000, come modificato dal DPR 137/2003.

In particolare, l'articolo 26 disciplinava l'attività dei certificatori, il 27 quella dei certificatori qualificati, il 28 dei certificatori accreditati, mentre il 29-bis e il 28-bis si incentrarono sulla responsabilità del certificatore.

Nella normativa precedente non era presente una definizione di certificato, cosi il contenuto del documento poteva determinarsi "par relationem" dalle definizioni di certificazione, di certificatore, di revoca, sospensione e di validità del certificato.

Nel Decreto 10/2002, art. 2, comma 1° lett. d), il legislatore definì il certificato elettronico come "l'attestato che collega i dati utilizzati per verificare la firma elettronica al titolare e conferma l'identità dei titolari stessi".

Quindi il certificato risultava fondamentalmente un documento informatico che aveva la funzione di confermare l'identità del titolare e di collegare i dati utilizzati per verificare la firma elettronica al titolare.

La disposizione non si riferiva direttamente alla chiave pubblica, perché il sistema di crittografia a chiavi asimmetriche non è necessariamente alla base del sistema di firme elettroniche. Tale sistema era tecnologicamente neutro, per cui poteva basarsi su tecniche tra loro molto diverse.

I certificati possono svolgere differenti funzioni ed essere di differente qualità.

Secondo la normativa italiana, i certificati si distinguono in:

- certificati elettronici, definiti come gli attestati elettronici che collegano

i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (art. 2, comma 1, lett. d) del D.Lgs. 23 gennaio 2002 n.10)

- certificati qualificati, definiti come certificati elettronici conformi ai requisiti di cui all'all. 1 della Direttiva 1999/93/CE che sono:

  1. l'indicazione che il certificato rilasciato è un certificato qualificato;
  2. l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;
  3. il nome del firmatario del certificato o uno pseudonimo identificato come tale;
  4. l'indicazione di un attributo specifico del firmatario, da includere, se pertinente, a seconda dello scopo per cui il certificato è richiesto;
  5. i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;
  6. un'indicazione dell'inizio e del termine del periodo di validità del certificato;
  7. il codice di identificazione del certificato;
  8. la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;
  9. i limiti d'uso del certificato ove applicabili;
  10. i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili; inoltre tali certificati devono essere rilasciati da certificatori che rispondono ai requisiti dell'all. 2 della medesima direttiva europea.

Quindi il primo tipo di certificato è un certificato semplice, mentre il secondo è caratterizzato da particolari requisiti. Sul primo tipo, il legislatore non si sofferma; la definizione è molto ampia e ha carattere generale. Sono

documenti informatici che hanno lo scopo di collegare i dati utilizzati per le firme elettroniche ai titolari e di confermarne l'identità.

Invece, i requisiti dei certificati qualificati sono dettagliatamente elencati all'articolo 27/bis del DPR 445/2000, come modificato dal DPR 137/2003. La norma riprende l'elenco dei requisiti dell'all.1 della direttiva europea.

L'articolo 3 del D.Lgs. 10/2002 apre il mercato dei certificatori e chiaramente dispone che l'attività dei certificatori stabiliti in Italia è libera e non soggetta ad autorizzazione preventiva.

Secondo il quadro normativo , i certificatori possono essere di più livelli :

- certificatori, senza ulteriore qualificazione, cui si applica l'art. 4 del D.Lgs. 10/2002 e l'art. 26 del DPR 445/2000, come modificato dal DPR 137/2003;

- certificatori che emettono certificati qualificati, cui si applica l'art. 4 del D.Lgs. 10/2002 e l'art. 27 del DPR 445/2000, come modificato dal DPR 137/2003;

- certificatori accreditati, cui si applica l'art. 5 del D.Lgs. 10/2002 e l'art.28 del DPR 445/2000, come modificato dal DPR 137/2003. Sono quelli che hanno ottenuto il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, e dotati di ulteriori requisiti, oltre a quelli richiesti per i certificatori che emettono i certificati qualificati.

Ovviamente, firme elettroniche, certificati e certificatori possono essere variamente combinati. Ad esempio, il certificatore accreditato può emettere anche certificati non qualificati, mentre il certificatore senza ulteriori qualificazioni non può emettere certificati qualificati.

2.3.1 Certificatori semplici

L'art. 26 del DPR 445/2000 stabilisce che l'attività i tali certificatori è libera e non necessita di autorizzazione preventiva, disposizione ripresa dall'art. 3 del D.Lgs. 10/2002.

Tuttavia, la norma fissa alcuni requisiti minimi, che sono quelli di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso istituti di credito di cui all'art. 26 D.Lgs. 385/1993.

Tali requisiti possono essere oggetto di successivi accertamenti, all'inizio dell'attività, per cui se viene verificata la mancanza dei detti requisiti, ciò comporta l'obbligo di cessazione dell'attività.

2.3.2 Certificatori qualificati

Questi certificatori che emettono certificati qualificati devono anche:

1. dimostrare l'affidabilità organizzativa, tecnica, e finanziaria per svolgere l'attività;

2. impiegare personale dotato delle conoscenze specifiche, esperienza e competenze necessarie;

3. applicare procedure e metodi amministrativi e di gestione adeguati a tecniche consolidate;

4. utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica;

5. adottare adeguate misure contro la contraffazione dei certificati, per garantire riservatezza, integrità e sicurezza nella gestione delle chiavi (art. 27, 2° comma lett. d) del DPR 445/2000, modificato dal DPR 137/2003).

Quindi i certificatori qualificati devono dimostrare la loro affidabilità, con riferimento al profilo organizzativo- gestionale e con riferimento alla sicurezza tecnica.

In particolare, il 2° comma, lett. d) del nuovo art. 27 del DPR 445/2000, modificato dal DPR 137/2003, rinvia a un decreto del Presidente del Consiglio dei Ministri o del Ministro per l'innovazione e le tecnologie avente come oggetto l'accertamento della conformità dei dispositivi sicuri per la creazione di una firma ai requisiti prescritti dall'allegato 3 della direttiva 1999/1993, in base a uno schema nazionale di valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione.

Risulta che, i certificatori qualificati prima dell'inizio dell'attività, devono dare notizia al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, che svolge funzioni di controllo dei requisiti dei certificatori qualificati.

Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici e privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente testo unico e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti. Ciò, salvo che l'interessato provveda a conformare alla normativa vigente l'attività e i suoi effetti entro il termine fissato dall'amministrazione stessa.

Poi, secondo il nuovo art. 29-bis, lett. m) del DPR 445/2000, modificato dal DPR 137/2003, il certificatore qualificato deve tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni, allo scopo di fornire prova della certificazione in eventuali procedimenti giudiziari.

Certificatori accreditati

Questi certificatori devono presentare domanda per accreditarsi al Dipartimento per l'innovazione e le tecnologie, presso la Presidenza del Consiglio dei Ministri ed essere iscritti in un apposito elenco (art. 28, comma 1, del DPR 445/2000, modificato dal DPR 137/2003).

L'accreditamento è il riconoscimento del possesso, da parte del certifi-

catore, dei requisiti del livello più elevato, che si possono impiegare sia nei rapporti con privati, sia con la PA.

Il richiedente deve allegare alla domanda il profilo professionale del personale responsabile della generazione dei dati per la creazione e la verifica della firma, dell'emissione dei certificati e della gestione del registro dei certificati, nonché l'impiego al rispetto delle regole tecniche (art. 28, comma 2, del DPR 445/2000, modificato dal DPR 137/2003) .

La domanda si considera accolta quando non venga comunicato all'interessato il provvedimento di diniego entro 90 giorni dalla data di presentazione (art. 28, comma 4, del DPR 445/2000, modificato dal DPR 137/2003).

A seguito dell'accoglimento della richiesta, il Dipartimento dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal Dipartimento stesso (art. 28, comma 6, del DPR 445/2000, modificato dal DPR 137/2003).

I requisiti stabiliti per le tre categorie di certificatori hanno l'intento di garantire una certa stabilità e permanenza nel tempo della struttura che deve possedere le autorità di certificazione per il delicatissimo ruolo da esse svolto, nonché per la responsabilità che è a esse attribuita.

Gli obblighi specifici del certificatore che sono esposti nell'art. 29-bis, 2° comma, possono essere ricondotti a funzioni diverse.

Secondo una classificazione universalmente accettata, le funzioni sono raggruppate in

- identificazione (registration service)
- certificazione (certification service), comprende la pubblicazione delle chiavi pubbliche e dei certificati
- altre funzioni, come la validazione temporale, volta a conferire a un documento informatico una data certa.

Il certificatore ha precisi obblighi di informazione nei confronti dei richiedenti e deve: "predisporre sui mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione , tra

cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in un linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il certificatore"[28].

Inoltre, come da lettera n) del suddetto decreto, è fatto divieto al certificatore di copiare o conservare le chiavi private del soggetto cui ha fornito servizi, poiché si troverebbe nella posizione di poter apporre la firma al posto del titolare.

Tra i vari obblighi di carattere generale che sono richiesti da regolamento, occorre ricordare quelli relativi al trattamento dei dati personali. La normativa sul trattamento dei dati personali è richiamata anche dal 3° comma dell'art. 29-bis del DPR 445/2000 come modificato dal DPR 137/2003, dove è esposto che: "il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato , fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono".

L'art. 28-bis disciplina la responsabilità del certificatore, recependo le disposizioni della direttiva europea (art.6). Innanzitutto, secondo quest'ultima, egli è responsabile nei confronti di terzi, dell'esattezza di tutte le informazioni contenute nel certificato. E può liberarsi da questo vincolo solo se dimostra di aver agito senza colpa.

Occorre sottolineare che la responsabilità del certificatore è molto forte: in sostanza si è in presenza della speciale responsabilità per attività pericolosa, di cui all'art. 2050 C.C. Il certificatore può indicare nel certificato i limiti d'uso e non rispondere dei danni derivanti dall'uso indebito. Analogamente

[28] Art. 29-bis, 2° comma, lettera o) del DPR 445/2000 come modificato dal DPR 137/2003

può indicare nel certificato un valore limite e non rispondere dei danni superiori a condizione che i limiti d'uso e il valore limite siano riconoscibili a terzi.

Inoltre, il certificatore è pienamente responsabile della piena osservanza dei requisiti previsti dalla direttiva riguardo al rilascio del certificato qualificato.

L'art. 28-bis disciplina i rapporti tra certificatore e terzi che abbiano fatto ragionevole affidamento sul certificato.

In particolare:

- sull'esattezza delle informazioni alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati;
- sulla garanzia che al momento del rilascio, il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui in certificatore generi entrambi.

Inoltre, la responsabilità del certificatore va riferita ai danni cagionati a chi faccia ragionevole affidamento sul certificato, all'esattezza delle informazioni contenute nel certificato, alla garanzia che al momento del rilascio detenesse i dati per la creazione della firma corrispondenti a quelli di verifica della firma, alla garanzia che i dati di creazione e di verifica della firma possano essere utilizzati in modo complementare.

Poi, riguardo ai danni cagionati a terzi che facciano ragionevole affidamento sul certificato stesso per la mancata registrazione della revoca o della sospensione del certificato, il certificatore risponde se non prova di aver agito senza colpa[29].

[29] Art. 28-bis del DPR 445/2000

Infine, spostiamo l'attenzione sulle firme elettroniche e la Pubblica Amministrazione.

Questa materia che, dopo la pubblicazione del DPCM 8 febbraio 1999, era stata oggetto di numerose discussioni, ha avuto una sua sistemazione nel febbraio 2001 con la circolare Aipa n.27 che ha fornito un inattesa soluzione chiara e organica.

Innanzitutto, viene fatta una distinzione tra documenti informatici con rilevanza esterna e quelli con rilevanza solo interna:

1. nel primo caso, ai fini della sottoscrizione ove prevista, le amministrazioni possono svolgere in proprio l'attività di certificazione, ma limitatamente ai propri organi ed uffici ed hanno l'obbligo di iscriversi nell'elenco pubblico dei certificatori, attenendosi alle regole tecniche del DPCM, oppure rilasciare certificati di firma digitale relativi ai propri organi ed uffici, avvalendosi dei servizi offerti dal Centro Tecnico della Presidenza del Consiglio dei ministri o dai certificatori iscritti nell'elenco di cui sopra, acquisiti nel rispetto della vigente normativa in materia di contratti pubblici; in questo caso non vi è obbligo di iscrizione nel citato elenco pubblico.

2. per la sottoscrizione di documenti informatici di rilevanza interna le amministrazioni possono rilasciare ai propri organi ed uffici firme elettroniche certificate secondo le regole tecniche diverse da quelle fissate dal DPCM.

A questo riguardo la circolare spiega: "la sottoscrizione prevista dal punto b) è finalizzata a soddisfare esigenze di semplificazione del processo di formazione dei documenti amministrativi, per quegli adempimenti di rilevanza esclusivamente interna, ritenendosi che l'impiego della firma digitale, come era prevista dal DPR 513/97, e ora regolata dalla normativa vigente prima esposta e dalle relative regole tecniche, contenute nel DPCM 8 febbraio 1999, determinerebbe un notevole appesantimento del processo documentale stesso.

Ogni amministrazione pubblica potrà prescindere dal formale processo di certificazione della chiave pubblica previsto dal DPR 513/97 e ora regolata dalla normativa vigente come sopra esposta e dal DPCM 8 febbraio 1999 e ricorrere a regole tecniche dalla stessa autonomamente definite, sia per la generazione e conservazione delle chiavi pubbliche che per la loro certificazione, limitatamente alla sottoscrizione dei documenti informatici d'uso interno e con riferimento al proprio ordinamento.

Per tali adempimenti, la deroga alle regole tecniche di cui al DPCM del 8 febbraio 1999 è motivata dalla circostanza che la verifica dell'autenticità ed integrità del documento informatico può avvenire attraverso il solo riscontro interno, grazie al processo di certificazione operato da ogni singola amministrazione".

Bisogna precisare che inizialmente la firma digitale pareva dover essere utilizzata sia dai pubblici che dai privati, ogni volta si procedesse alla sottoscrizione di documenti informatici.

In seguito, uno studio più attento della norma ha reso chiaro che l'applicazione della firma "forte" poteva essere limitata nei soli casi in cui il documento era destinato ad avere valore legale esterno. Ne consegue che, nelle applicazioni interne, non era necessario ricorrere alla firma forte.

I concetti di rilevanza esterna e rilevanza interna sono stati rielaborati nelle norme successive. Infatti nel T.U. all'articolo 29-quinquies, commi 1 e 2, si legge "

1. ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

    - possono svolgere direttamente l'attività di rilascio di certificati qualificati, avendo a tal fine l'obbligo di accreditarsi ai fini dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici e privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti

con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto;

- possono rivolgersi a certificatori accreditati secondo la vigente normativa in materia di contratti pubblici.

2. per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 8, comma 2".

Quindi, all'interno, ogni amministrazione potrà adottare un sistema di firma qualificato senza che il certificatore sia accreditato, oppure un sistema autonomo tipo PGP.

C'è ancora qualche perplessità nel capire come potrà convivere nella stessa amministrazione un sistema informatico di firma solo per l'interno con uno solo per l'esterno.

2.4 La Firma digitale nel CAD 2005

Il Decreto Legislativo n. 82 del 7 marzo 2005[30] reca il Codice dell'Amministrazione Digitale, emanato ai sensi della "Legge di semplificazione 2001"[31], il cui articolo 10 aveva per oggetto il riassetto in materia di società dell'informazione.

l Codice, che venne adottato in via definitiva dal Consiglio dei Ministri nella seduta del 4 marzo 2005, rappresentò un documento complesso e ambizioso, visto le materie che ha disciplinato e che intervenne a sistematizzare in materia di governo elettronico.

[30]Decreto Legislativo del 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale, pubblicato nella Gazzetta ufficiale n. 112 del 16 maggio 2005

[31]Legge del 29 luglio 2003, n. 229, Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – Legge di semplificazione 2001, pubblicata nella Gazzetta ufficiale n. 196 del 25 agosto 2003.

Il Codice entrò in vigore il 1 gennaio 2006. Ebbe lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione all'interno della PA, nei rapporti tra amministrazione e privati e in alcuni limitati casi, disciplinò anche l'uso del documento informatico nei documenti tra privati.

Il codice si componeva tre grandi parti:

- La prima, che stabiliva i principi generali della nuova Pubblica Amministrazione digitale e i nuovi diritti in capo ai cittadini ed alle imprese.

- La seconda parte, riguardante gli strumenti che rendevano possibile la realizzazione dell'attività amministrativa informatizzata e la loro validità giuridica.

- La terza, infine, avente per oggetto le modalità, i tempi, le responsabilità e i ruoli per realizzare questa trasformazione.

L'emanazione del Codice suscitò impressioni contrastanti presso gli osservatori e presso la dottrina giuridica anche perché rappresentava una novità dal momento che fu abbandonato il metodo del Testo Unico.

Da un lato, erano presenti coloro che ne accolsero positivamente l'uscita, considerandolo un importante atto di riordino della materia.

Dall'altro lato, una parte affatto minoritaria della dottrina, si mostrò alquanto scettica sulla effettiva portata innovativa del decreto, per diverse ragioni. In primo luogo, perché il Codice si componeva di numerose enunciazioni di principio, spesso piuttosto solenni, senza l'accompagnamento però di disposizioni operative che ne rendano effettiva l'attuazione.

In secondo luogo, perché avrebbe scorporato un assetto normativo che già era organico: la disciplina del documento informatico, secondo tale opinione, trovava infatti la propria sede naturale nel "testo unico sulla documentazione

amministrativa"[32], dove l'atto elettronico era disciplinato contestualmente all'atto cartaceo in un regime di perfetta alternativa tra i due supporti.

Infine, secondo la dottrina più scettica, con il "codice" sarebbe degenerato l'intento iniziale di usare l'informatica come strumento per la semplificazione amministrativa, facendo diventare la digitalizzazione un fine a sé stante. Si sarebbero così sottovalutati i rischi di un passaggio non sufficientemente graduale dal cartaceo all'elettronico, primo fra tutti quello dell'acuirsi del digital divide fra cittadini dotati di confidenza con lo strumento informatico, e cittadini che per ragioni sociali o anagrafiche hanno difficoltà a rapportarsi telematicamente con l'amministrazione.

2.4.1 Il documento informatico nel CAD 2005

Nell'articolo 1 sono contenute le varie definizioni degli elementi coinvolti in questa disciplina.

"Art. 1, lettera p: (*documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti) ;*"

La formulazione era identica a quella dei precedenti testi normativi. Nel linguaggio giuridico relativo ai documenti creati attraverso la tecnologia informatica, i termini informatico ed elettronico furono intesi come sinonimi.

Sotto il profilo strettamente tecnico, il documento informatico era il prodotto di un elaborazione mediante computer e, in senso stretto, redatto e conservato sotto forma di bit su supporti diversi, come ad esempio nelle memorie ausiliarie attraverso la magnetizzazione o smagnetizzazione del supporto, oppure attraverso un processo di formazione o meno di buchi nella superficie magnetica della memoria ausiliaria con un raggio laser.

Ad ogni modo l'articolo citato confermava la rilevanza giuridica del documento informatico ed, in particolare, l'equivalenza giuridica tra documento cartaceo e documento informatico.

La definizione di documento informatico riproposta nel Codice assumeva un significato fortemente innovativo in merito al possibile "contenuto" dello

[32]DPR 445/2000

stesso, soprattutto per quanto concerne la sua stessa struttura . Tale definizione si discostava dalla tradizionale definizione di documento giuridico come res rappresentativa di un fatto giuridicamente rilevante .

Facendo riferimento in modo esplicito a fatti, atti e dati, si prospettava una puntuale tipologia dei possibili contenuti del documento, la quale teneva conto di quella peculiare capacità rappresentativa dei mezzi informatici che moltiplicano le numerose possibilità e modalità del documentare.

L'ulteriore e più rilevante specificità della disposizione normativa riguardava però la struttura del documento stesso. Infatti, l'articolo omette ogni riferimento al supporto che registra il contenuto del documento. Proprio questa specificità ha contribuito alla nascita di teorie che sottolineano la "natura immateriale" del documento informatico.

Facendo riferimento alla disposizione citata del Codice, queste teorie affermavano che il documento informatico "vive" indipendentemente dal supporto che lo contiene. Esso è un "documento immateriale" in quanto non incorporato in un supporto materiale.

Nell'era della immaterialità e della virtualità ci sembra legittimo che venisse sancita a livello legislativo, una nozione di documento informatico come mera rappresentazione di dati del tutto autonoma e svincolata dal supporto sul quale questi dati vengono di volta in volta memorizzati.

La validità giuridica di un documento informatico è condizionata all'osservanza di un insieme di prescrizioni riguardanti sia la formazione dello stesso, sia la sua trasmissione telematica. Un documento informatico, infatti, benché formato nel rispetto delle prescrizioni dettate sulla formazione del documento medesimo, potrebbe non essere considerato giuridicamente equivalente al corrispondente documento cartaceo e per tanto, qualora la sua trasmissione telematica non rispetti le disposizioni vigenti, privo di valore giuridico.

Le prescrizioni concernenti la formazione e la trasmissione telematica del documento informatico sono state sintetizzate nel Codice all'articolo 20, primo comma, così come modificato ed integrato dal Decreto Legislativo n. 159/2006.

Art. 20, 1° comma: (Il documento informatico da chiunque formato, la registrazione su supporto informatico e la sua trasmissione con strumenti telematici [...] sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente Codice.)

Per quanto riguarda la disciplina sulla realizzazione di documenti informatici, bisogna innanzitutto fare la distinzione tra due categorie di norme. Da un lato la disciplina dei documenti la cui validità giuridica è condizionata al rispetto di certe prescrizioni, che se osservate consentono l'equiparazione tra documento informatico e documento cartaceo, dall'altro la disciplina dei documenti informatici che attribuisce ad essi validità giuridica a prescindere dall'equivalenza giuridica con i corrispondenti documenti cartacei.

In quest'ultimo caso ci sono state disposizioni ad hoc dettate per il documento informatico, questo insieme di norme interessava però solo alcuni tipi di documenti informatici. Nelle restanti ipotesi, in via residuale, si assumeva che la realizzazione dei documenti informatici si dovesse basare sulle disposizioni che rendevano giuridicamente equivalenti il documento informatico e il corrispondente documento cartaceo.

La regola fondamentale di tale equivalenza si trovava nell'articolo 20, secondo comma del Codice, così come integrato e modificato dal Decreto Legislativo 159/2006.

Art. 20, 2° comma: (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, primo comma, numeri da 1 a 12 del codice civile).

Questa formulazione mise un segno tangibile di una sensibile inversione di tendenza rispetto alla disciplina previgente. Infatti, come abbiamo visto, l'articolo 10 del Testo Unico aveva previsto che il requisito legale della forma

scritta fosse soddisfatto dal documento informatico sottoscritto con qualsiasi firma elettronica, prescindendo dalla tipologia di firma utilizzata e dal relativo grado di sicurezza. Ricordiamo che per questo motivo la dottrina aveva sollevato non poche critiche.

In modo ancora più chiaro, e per questo ancor più criticato, il d.lgs. 10/2002, nell'attuazione della Direttiva 1999/93/CE, aveva confermato il principio di "non discriminazione" tra documento informatico e documento su supporto cartaceo.

Il Codice ha avuto, senza dubbio, il merito di togliere di mezzo le improvvide modifiche introdotte con il DLgs 10/2002 e di ritornare alla disciplina antecedente. La nuova formulazione non ho compiuto tuttavia passi avanti e non mise fine alle controversie interpretative che hanno diviso i giuristi sui diversi aspetti della disciplina.

La dottrina risultava infatti divisa in due correnti. Da una parte, i sostenitori della tesi secondo cui solo il documento informatico provvisto di firma digitale qualificata era sinonimo di sicurezza ed affidabilità e poteva quindi avere valore giuridicamente vincolante. Dall'altra parte, coloro i quali affermavano che fosse assolutamente necessario garantire un'esistenza giuridica ai documenti informatici non sottoscritti o sottoscritti con firma elettronica semplice, al fine di garantire le transazioni del commercio elettronico.

Abbiamo già considerato gli aspetti negativi dell'ipotesi prevista dal Decreto Legislativo 10/2002, ora considereremo quelli della tesi del Codice. Innanzitutto il fatto di imporre agli operatori l'onere di scambiarsi unicamente documenti sottoscritti con firma elettronica qualificata o con firma digitale, almeno quando si necessitava di forma scritta, rendeva certamente più farraginose e complesse le transazioni del commercio elettronico. In questo modo, l'impostazione recepita nel Codice costituiva un forte elemento di rottura rispetto all'orientamento che andava diffondendosi tanto in ambito nazionale e internazionale, secondo cui la sottoscrizione autografa era considerata incompatibile con le tecnologie di comunicazione e con le esigenze di rapidità degli affari.

Di fatto, il mancato riconoscimento dell'idoneità a rivestire la forma scritta dei documenti informatici non sottoscritti, o in ogni caso sottoscritti con la firma elettronica semplice, non teneva conto delle "ragioni del progresso" e limitava l'agire dei privati nella attuale società dell'informazione.

In seguito alle modifiche e alle integrazioni apportate con il Decreto Legislativo n. 159/2006, il legislatore introdusse un altro comma all'articolo 20, dimostrando una certa consapevolezza riguardo ai problemi affrontati poco sopra.

Art. 20, comma 1-bis: (1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21).

La nuova disposizione in qualche modo incise sulla capacità satisfattiva dei documenti informatici sprovvisti di firma digitale, o di altra firma elettronica qualificata, a soddisfare il requisito della forma scritta. Sembra evidente che l'intento perseguito dal legislatore in sede di riforma, sia stato proprio quello di ampliare il novero dei documenti informatici in grado di soddisfare il requisito della forma scritta, probabilmente con il fine di salvaguardare le prassi riscontrate nella contrattazione on-line, a partire dalle e-mail, le quali di fatto sono state dettate da esigenze di rapidità e celerità incompatibili con l'uso della firma digitale.

L'introduzione di questo comma sembrava risolvere il problema di coordinamento che si poneva con la disposizione di cui all'articolo 45 del Codice.

Art. 45: I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

Risulta evidente che nell'assenza di uno specifico richiamo sul valore giuridico della firma elettronica semplice e riconoscendo nell'articolo 45 la rile-

vanza di forma scritta anche a quei documenti trasmessi per mezzo telefax, si introduceva il principio incompatibile con quello espresso nell'originaria formulazione dell'articolo 20, il quale testualmente riconosceva rilevanza di forma scritta ai soli documenti sottoscritti con firma qualificata o digitale, presupponendo un'identificazione del mittente certa e sicura.

Questi dubbi di coordinamento tra articolo 20 e articolo 45 sono stati risolti dall'introduzione del comma in esame. Infatti, nelle ipotesi di controversie riguardanti i documenti informatici non sottoscritti o sottoscritti con firma elettronica semplice,fu stabilita l'autorità del giudice nel valutare liberamente l'idoneità a soddisfare il requisito della forma scritta *tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità, ed immodificabilità.*

Se risultava pacifico che la sottoscrizione non dovesse necessariamente essere autografa, ma anche rappresentata da altri segni che egualmente ne comprovino l'identità della persona e la sua volontà di far propria una dichiarazione, sfruttando tutte le prestazioni di cui è suscettibile un computer, sarebbe stato opportuno che il legislatore avesse previsto una qualsiasi forma di sottoscrizione, almeno in vista di quella "funzione di responsabilizzazione del consenso" che era ormai stata assunta in dottrina, nella quale è rinvenibile sia che il soggetto apponga la sua firma autografa al documento cartaceo, sia laddove sia sostituita da procedure informatiche intese a far risultare l'identità del dichiarante e la sua volontà di rispondere della dichiarazione medesima. Ne conseguiva che, se pur apprezzabile la scelta di aver ridato asilo giuridico a documenti sprovvisti di firma digitale, appariva eccessiva la soluzione adottata nel comma 1-bis dell'attuale articolo 20, laddove, sempre ai fini di valutare la rilevanza della forma scritta , scomparve qualsivoglia riferimento alle diverse tipologie di sottoscrizione elettronica, che avrebbe avuto modo di essere mantenuta.

2.4.2 La firma digitale nel CAD 2005

La disciplina della sottoscrizione informatica contenuta nel Codice riprendeva sostanzialmente la normativa precedente, sebbene per alcuni profili

apportò qualche modifica.

La modifica più importante riguardava la riduzione del numero delle firme. Come abbiamo visto, prima del 2005, era possibile individuare quattro tipi di firme informatiche: la firma digitale, quella elettronica semplice, avanzata e qualificata. A queste si aggiungevano tre strutture di certificazioni e due tipi di certificato. Alla loro combinazione, il legislatore associava un diverso valore giuridico e una diversa efficacia probatoria.

Il codice ha il merito di aver razionalizzato la materia, prevedendo due sole tipologie di firme: quella "semplice" e quella "qualificata". La firma digitale si presentava come specificazione di quest'ultima. Ci sembra opportuno tornare alle definizioni di cui all'articolo 1 del Codice.

Art. 1, lettera q: *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;*

Art. 1, lettera r: *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;*

Come abbiamo visto, la firma digitale non è altro che una species del genus firma elettronica qualificata, ma si tratta anche del tipo di firma elettronica più affidabile prevista dal Codice.

Probabilmente per questo motivo, la disciplina dettata al Capo II riguarda quasi esclusivamente la firma digitale. Al contrario, non si rivela alcuna disposizione intitolata ed indirizzata alla disciplina della firma elettronica semplice e della firma elettronica qualificata.

Si aggiunga che la concreta possibilità di servirsi della sottoscrizione informatica è favorita, se non condizionata, dall'emanazione della regolamentazione tecnica. Appresa infatti la definizione di una determinata tipologia

di sottoscrizione informatica, al livello attuativo occorre fare riferimento ad una serie di regole di natura tecnico-informatica che non sono contenute nel Codice. La disciplina tecnica in materia all'epoca era quella contenuta nel d.p.c.m. 13 gennaio 2004, che riguarda esclusivamente le firme digitali.

Ai sensi dell'articolo 71 del Codice le nuove regole tecniche avrebbero dovuto essere emanate entro nove mesi dalla data di entrata in vigore del decreto. Questo articolo però, non chiariva se esse avrebbero dovuto riguardare anche le tipologie di firma elettronica diverse dalla firma digitale.

Art. 1, lettera s: *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;*

L'apposizione della firma digitale è giuridicamente equivalente alla sottoscrizione autografa.

Essa inoltre, in base all'articolo 24, secondo comma, sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

2.4.3 Il valore legale dei documenti informatici

Il valore legale di un documento informatico dipendeva, come detto, dal tipo di sottoscrizione. Il riferimento chiave era l'articolo 21 del Codice, integrato e modificato dal decreto legislativo 159/2006.

Art. 21: *Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.*

Art. 21, 2° comma: *Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria.*

Il documento informatico sottoscritto, pertanto, assumeva un duplice valore probatorio: costituiva prova semplice oppure valore di prova legale.

A livello processuale, la prova semplice poteva essere contestata ricorrendo alla mera prova contraria. La prova legale, invece, era contestabile soltanto ricorrendo alla querela di falso ex articoli 2699 e 2702 del codice civile, salvo disconoscimento della sottoscrizione (art. 2702 c.c.).

L'attendibilità della prova semplice era affidata al libero apprezzamento del giudice, l'attendibilità della prova legale, invece, veniva stabilita a priori dalla legge. Nell'ambito delle prove documentali veniva riconosciuto valore probatorio pieno (prova legale) all'atto pubblico (art. 2699 c.c.) e alla scrittura privata (art. 2702 c.c.).

Per quanto riguarda i documenti informatici si necessita di una distinzione tra valore probatorio pieno, che implica il ricorso alla sottoscrizione digitale o ad altro tipo di sottoscrizione elettronica qualificata, e il valore probatorio semplice, che implica il ricorso alla firma elettronica semplice.

L'efficacia probatoria delle diverse fattispecie di documento informatico che il nostro ordinamento ha contemplato può essere riassunta nei seguenti termini:

Il documento informatico sottoscritto mediante una firma elettronica semplice dava prova semplice dei fatti e delle circostanze in esso allegate secondo la libera valutazione del giudice, che tuttavia poteva essere condizionata dall'apprezzamento delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento elettronico.

Il documento informatico sottoscritto mediante firma digitale o con altro tipo di firma elettronica qualificata invece forniva piena prova della provenienza delle dichiarazioni di chi l'ha sottoscritto, come previsto dal secondo comma dell'articolo 21. Il Codice attribuiva così valore probatorio pieno al documento informatico sottoscritto con la così detta firma forte, ossia quella digitale o qualificata, stabilendo un'equivalenza giuridica rispetto all'efficacia probatoria della scrittura privata di cui all'articolo 2702 del codice civile. La scrittura privata fa piena prova fino a querela di falso della provenienza

delle dichiarazioni da chi l'ha sottoscritta, ma non dell'autenticità dell'atto documentato, se colui contro il quale la scrittura è prodotta ne riconosceva la sottoscrizione, ovvero se la scrittura risultava legalmente considerata come riconosciuta, in relazione all'apposizione di una sottoscrizione autenticata ai sensi dell'articolo 2703 del codice civile.

Tuttavia, se nella disciplina del codice civile, oltre alla querela di falso, era possibile operare il disconoscimento di firma relativo ai documenti cartacei, per effetto delle disposizioni del Codice l'utilizzo del dispositivo sicuro di firma, si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

Fu introdotta una presunzione che il sottoscrittore apparente poteva superare solamente fornendo la prova contraria. Si trattava quindi della presunzione relativa che il titolare del dispositivo di firma era colui che sottoscriveva il documento.

Questa presunzione operava sia a favore di chi produceva il documento in giudizio, dal momento che questo era dispensato dall'onere di provare che era stato effettivamente il titolare ad utilizzare materialmente il dispositivo di firma, sia a favore dello stesso titolare, nella misura in cui gli consentiva di liberarsi degli effetti di un utilizzo abusivo del dispositivo dando prova, con qualsiasi mezzo, che l'utilizzo non è a lui riconducibile.

In ordine a tale disciplina si pronunciò criticamente il Consiglio di Stato (Sez. C del 30 gennaio 2006, n.31) che confrontò la normativa in esame con quella prevista dal diritto comunitario. Quest'ultimo, come sappiamo, imponeva agli Stati membri di equiparare, per quanto concerne gli effetti probatori, la firma autografa alla firma elettronica avanzata, basata su un certificato qualificato e generata con un dispositivo di firma sicuro.

Il Consiglio di Stato sottolineò che le disposizioni integrative e correttive introdotte nel tessuto del Codice dovevano rafforzare particolarmente sotto il profilo probatorio il valore legale del documento informatico sottoscritto con firma elettronica forte, a scapito del documento formato sul tradizionale supporto cartaceo. Secondo il Consiglio di Stato la parità di condizione

era apparente, perché l'efficacia probatoria della scrittura informatica veniva rafforzata dalla maggiore difficoltà del disconoscimento giudiziale della firma.

Infatti, colui contro il quale veniva esibita in giudizio una falsa scrittura cartacea poteva limitarsi a disconoscere la propria firma, dando luogo alla speciale procedura di verificazione, ex articoli 314 e seguenti del codice di procedura civile, nella quale colui che intendeva utilizzare la scrittura doveva anche provarne l'autenticità.

Invece, la parte processuale contro la quale veniva esibita in giudizio una falsa scrittura formata su supporto informatico, oltre a disconoscere la propria firma era tenuto anche fornire le prove della sua falsità, con un inversione dell'ordine probatorio non giustificato secondo la Corte.

Il supremo consesso amministrativo ha ritenuto che in questo modo quando il documento informatico veniva sottoscritto con firma elettronica forte, poneva come una via di mezzo tra scrittura privata e atto pubblico, dal momento che aveva in giudizio la stessa efficacia probatoria di una scrittura privata munita di sottoscrizione legalmente riconosciuta, ma che in realtà era semplicemente una scrittura privata munita di sottoscrizione non autenticata. In merito a tali critiche, tuttavia, il legislatore non ha ritenuto opportuno seguire il parere del Consiglio di Stato e di fatto non ha apportato modifiche rilevanti sul tema in questione, probabilmente perché temeva possibili disconoscimenti fraudolenti da parte di chi aveva affidato il proprio dispositivo di firma ad un terzo, infatti malgrado questo fosse espressamente vietato dal Codice[33], il testo non prevedeva alcuna sanzione.

Ultimo tema da prendere in considerazione con riguardo al tema in esame è il valore probatorio del documento informatico non sottoscritto. Il Codice non faceva riferimento all'efficacia probatoria del documento informatico non sottoscritto, salvo volerlo recuperare nell'articolo 23, primo comma, che in integrazione dell'articolo 2712 del codice civile, riconosceva al documento informatico non sottoscritto la stessa efficacia probatoria delle riproduzioni meccaniche riguardo ai fatti ed alle cose rappresentate sempre che colui con-

[33] Art. 32 del CAD

tro il quale veniva prodotto non ne disconoscesse la conformità all'originale. In tal senso, non è mancata in dottrina l'opinione di chi riconosceva nelle disposizioni in commento l'effetto di attribuire alla riproduzione informatica un'efficacia probatoria maggiore rispetto a quella del documento informatico da cui veniva trattata. In effetti, se era possibile che una riproduzione meccanica, nel caso in cui non veniva disconosciuta, forniva piena prova dei fatti e delle cose rappresentate, un'analoga previsione non è stata inserita nel Codice con riferimento ai documenti informatici sottoscritti elettronicamente, con la conseguenza che, questi ultimi, avevano un'efficacia probatoria condizionata dal prudente apprezzamento del giudice.

Ne conseguiva che la disciplina riguardante l'efficacia probatoria del documento informatico rischiava di rimanere esposta inesorabilmente ai mutevoli orientamenti giurisprudenziali, destinati peraltro a formarsi in un ambiente nel quale tardava ad affermarsi la cultura informatica.

Domandare al giudice valutazioni come quelle previste dall'articolo 21 del Codice, nell'assenza di adeguati parametri di giudizio significava mettere a rischio il principio della certezza del diritto e, per questa via, disincentivare gli operatori a servirsi delle nuove tecnologie nella propria attività d'impresa.

2.5 Le firme elettroniche e digitali nel testo del CAD 2010

La riforma nasce dalla convinzione che la digitalizzazione dell'azione amministrativa sia una vera e propria funzione di governo, imperniata sui principi di effettività e risparmio, e che realizza i maggiori benefici nei settori sanità e giustizia.

La sua adozione consentirà un'importante riduzione dei costi e un forte recupero di produttività.

"Si stima una riduzione dei tempi fino all'80% per le pratiche amministrative e, per effetto della dematerializzazione, un risparmio del 90% dei costi

della carta (circa 6 milioni di euro annui)."[34] [urlc]

L'introduzione di una nuova riforma in ambito digitale nelle PA è stata necessaria anche per il rispetto del piano E-GOV 2012, il quale definisce un insieme di progetti di innovazione digitale che, nel loro complesso, si propongono di modernizzare, rendere più efficiente e trasparente la PA, migliorare la qualità dei servizi erogati a cittadini e imprese e diminuire i costi per la collettività. L'orizzonte temporale è, appunto, quello stabilito del 2012, e in ragione di questo, il decreto legislativo prenderà efficacia immediata per avviare il processo di digitalizzazione delle PA in contemporanea a quello di sburocratizzazione.

Un altra ragione dell'essere del nuovo CAD è da ricercare nella scarsa evoluzione normativa: il vecchio Codice dell'amministrazione digitale ha visto la nascita nel 2005, quindi ormai più di cinque anni fa, e come prevedibile, in questo lasso di tempo le tecnologie si sono rapidamente evolute, rendendo necessarie modifiche al testo normativo.

I principi ispiratori del nuovo testo sono due: primo, la ricerca di un impiego effettivo, offrendo incentivi alle amministrazioni che attueranno piani di utilizzo dei nuovi strumenti, e sanzioni a tutte le altre "dormienti"; secondo, l'informatizzazione dei processi e la razionalizzazione delle organizzazioni, ovvero snellire i processi, incentivare il personale alle nuove tecnologie e riutilizzo dei risparmi derivanti dall'impiego di queste ultime.

Il D.Lgs. n. 82 del 7 marzo 2005, contenente il Codice dell'amministrazione digitale (CAD), è stato modificato e integrato dal D.Lgs. n. 235 del 30 dicembre 2010. Iniziamo l'esame dell'articolato del rinnovato Codice, dunque, partendo da uno degli strumenti più importanti in esso disciplinati, la firma digitale, in modo da individuare le principali novità rispetto alla disciplina precedente.

Art. 1: definizioni

Nella nuova definizione di firma digitale cambia l'inquadramento di ge-

[34] Da www.padigitale.it

nere: la firma digitale non è più un particolare tipo di firma elettronica qualificata, ma di firma elettronica avanzata.

Nell'incrocio delle tre definizioni si perde, a livello definitorio, il riferimento della firma digitale al dispositivo sicuro, contenuto solo nella definizione di firma elettronica qualificata.

Inalterate rimangono le definizioni di chiave privata e chiave pubblica, nonché di certificato qualificato, tutti connessi alla firma digitale che, pertanto, già a livello definitorio, continua ad essere l'unico tipo di firma elettronica legata ad una determinata tecnologia.

Art. 20: documento informatico

Trattandosi di un articolo dedicato al documento informatico non sottoscritto, è stato opportunamente abrogato il comma 2, che riguardava appunto il documento informatico sottoscritto con firma digitale.

Nel comma 3 sono stati inseriti, invece, i riferimenti di rinvio alle regole tecniche sulle firme elettroniche avanzate che, per ragioni di coerenza sistematica, avrebbero potuto essere collocati più opportunamente nell'articolo successivo (analogamente si potrebbe sostenere per il rinvio alle regole tecniche sulla validazione temporale).

Art. 21: documento informatico sottoscritto con firma elettronica

Il comma 2 cambia con l'aggiunta delle firme elettroniche avanzate e dei riferimenti alle regole tecniche (mutuati dal precedente art. 20): pertanto, il documento informatico sottoscritto anche con firma elettronica avanzata, e non più soltanto qualificata o digitale, ha l'efficacia di cui all'art. 2702 c.c.

Per quanto concerne il rinvio alle regole tecniche, crediamo si sia persa l'occasione di eliminare l'ambiguità del tipo di riferimento, già contenuto nel testo precedente: infatti, la norma dispone, come prima, che il documento con firma digitale abbia la suddetta efficacia, purché sia formato nel rispetto delle regole tecniche "che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento". Ciò presuppone che vi possano essere regole tecniche che non garantiscano tali indispensabili requisiti, altrimenti tale riferimento non avrebbe significato o, quanto meno, sarebbe del tutto

superfluo. Poiché non sono ammissibili regole tecniche che non garantiscano ciò che la legge loro impone, né si può ipotizzare una estemporanea valutazione di idoneità delle regole tecniche a soddisfare i predetti requisiti, riteniamo che questo riferimento sia da eliminare.

La superiore dignità della firma digitale riemerge nel nuovo comma 2 bis, ove le scritture private di cui all'art. 1350 c.c., primo comma, numeri da 1 a 12, se fatte con documento informatico, devono essere sottoscritte con firma digitale (o qualificata); rimane salva l'eccezione di cui al successivo art. 25.

Art. 24: firma digitale

Nessuna novità in questo articolo: la firma digitale, pertanto, continua a riferirsi univocamente a un solo soggetto e a un documento o insieme di documenti, ed è imprescindibilmente subordinata alla validità e completezza del certificato qualificato, secondo quanto disciplinato nelle relative regole tecniche.

Art. 25: firma autenticata

La rilevante novità consiste nell'aver allargato l'area delle firme autenticabili, sganciandole dalla necessaria sussistenza di un certificato qualificato (o addirittura da qualsivoglia certificato elettronico). Nel precedente testo l'autenticazione poteva avere ad oggetto solo la firma digitale o elettronica qualificata, con una verifica del relativo certificato da parte del notaio. La nuova autenticazione, invece, può riguardare qualsiasi firma elettronica, inclusa l'acquisizione digitale della sottoscrizione autografa. D'altro canto, il nuovo art. 52 bis della legge 89/1913 (come introdotto dal D.Lgs. n. 110/2010 sull'atto pubblico informatico notarile) ha già previsto che la parti possano sottoscrivere l'atto pubblico informatico, in presenza del notaio, anche con una semplice firma elettronica consistente nell'acquisizione digitale della sottoscrizione autografa. Occorre rilevare, inoltre, che il nuovo art. 68 bis della legge 89/1913 rimanda a successivi decreti per individuare le tipologie di ulteriori firme elettroniche che potranno essere utilizzate per la firma dell'atto pubblico. In mancanza di tali decreti, l'area di tali firme elettroniche non appare concretamente identificabile; analogamente potrebbe

ritenersi per le firme elettroniche prive di certificato qualificato o elettronico di cui all'art. 25 del nuovo CAD.

Art. 35: dispositivi sicuri e procedure per la generazione della firma

Nel nuovo comma 3 si ammorbidisce il requisito di validità delle firme con procedura automatica: scompaiono i riferimenti alla "chiara riconducibilità alla volontà del titolare" e al "singolo documento", che sono sostituiti da un generico "previo consenso" del titolare all'adozione della procedura automatica.

Art. 65: istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

L'art. 65 prevede una elencazione di strumenti informatici che conferiscono validità alle suddette istanze e dichiarazioni. Tra questi strumenti, la firma digitale figura al primo posto: nessun cambiamento su questo punto. La novità risiede nell'eliminazione della facoltà, per la pubblica amministrazione, di stabilire i casi in cui è necessaria la firma digitale (in luogo o in aggiunta agli altri strumenti). A seguito del nuovo comma 1 bis, infatti, sarà un decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa ad individuare i casi in cui sarà necessaria la firma digitale.

Dunque, al momento in Italia esistono ben quattro tipologie di firma elettronica: la firma elettronica, la firma elettronica avanzata, la firma elettronica qualificata e la firma digitale (queste ultime due firme costituiscono un sottoinsieme della firma elettronica avanzata). Inoltre, dalla lettura delle definizioni, la firma digitale non coinciderebbe più con la firma elettronica qualificata in quanto, nella definizione della firma digitale, non c'è traccia del dispositivo sicuro di firma (requisito ancora essenziale per la firma elettronica qualificata). Si potrebbe trattare di una "semplificazione" generata dalle tecniche del legiferare moderno, dove troppo spesso vi è la tendenza alla modifica in base alle vecchie leggi, senza dare un effettivo sguardo alle esigenze future.

Inoltre, se nel nuovo assetto normativo il dispositivo sicuro di firma do-

vesse ritenersi un requisito superfluo per la firma digitale (e per la firma elettronica avanzata), come si spiegherebbe il contenuto dell'art. 21 comma 2[35][urld], secondo il quale per tutte le tipologie di firma (digitale, qualificata e avanzata) "*l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*" Suonerebbe come un controsendo degno di una commedia, ovvero bisogna dare prova contraria, ma senza avere i reali mezzi per farlo effettivamente. Infine, ad oggi la firma elettronica avanzata non esiste e non corrisponde alla "firma elettronica biometrica". La firma elettronica avanzata è definita in modo contorto nel CAD come *"l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati".*

Sempre secondo l'art. 21, tale tipologia di firma garantirebbe al documento informatico, allo stesso modo della firma elettronica qualificata e della firma digitale, l'efficacia prevista dall'articolo 2702 del codice civile, purché sia formata nel rispetto delle regole tecniche. Ma l'effettiva presenze delle suddette regole è ancora da ricercare, ovvero non ci sono.

Quindi, senza regole tecniche, la firma elettronica avanzata non esiste e la firma biometrica va utilizzata con la massima attenzione, deve essere giustificata, può essere al massimo accostata ad una firma elettronica semplice e ogni volta va verificata la sua utilizzabilità nel rispetto del Codice per la protezione dei dati personali.

Degno di nota è anche il comma 2 dell'art. 23-ter che, facendo riferimento alla firma elettronica avanzata, precisa che *"i documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile". Peccato che non è stato toccato dalla riforma il comma*

[35]Fonti:www.saperi.forumpa.it

2 dell'art. 34, secondo il quale "per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71". Ovvero, se nei procedimenti interni le Pubbliche Amministrazioni possono liberamente muoversi nella loro autonomia organizzativa risulta poco comprensibile il riferimento alla firma elettronica avanzata contenuto nell'art. 23-*ter*.

Sempre in tema di firme, va segnalata anche l'introduzione del GLIFO, novità del CAD. Il comma 5 dell'art. 23-*ter* specifica che *"al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico".*

Singolare è il fatto che non esistono tracce di regole tecniche in merito, ma che in realtà la reale funzione di questo sistema introdotto, sia quello di poter stampare documenti informatici direttamente da siti web istituzionali, non permettendo cosi il processo di dematerializzazione. Questa funzione è stata resa tale da varie PA che hanno cercato di dare un senso al suddetto strumento.

In conclusione riporto un articolo molto ben strutturato dalla Prof. Giusella Finocchiaro, la quale spiega le definizioni delle varie firme informatiche, l'efficacia probatoria, il valore giuridico, le modifiche in corso, e in generale cosa cambia tra il CAD 2005 è quello attuale.

Da http:www.blogstudiolegalefinocchiaro.it:"Le Commissioni Affari Costituzionali di Camera e Senato hanno espresso parere favorevole sulla proposta di riforma di CAD. Fra le modifiche apportate al Cad dalla bozza in circolazione, si devono segnalare l'introduzione della firma elettronica avanzata e la modifica delle norme sull'efficacia probatoria e sulla forma scritta.

Spiegare le definizioni delle varie firme informatiche, l'efficacia probatoria, il valore giuridico e le modifiche in corso è complicato. Ci provo. Ma non pretendo di riuscirci con un solo post. D'altronde il tema è caldo e c'è davvero tanta confusione....

1)Quante saranno i tipi di firme informatiche se verrà approvata la modifica al CAD oggi in circolazione?

Quattro: firma elettronica, firma elettronica avanzata, firma elettronica qualificata, firma digitale.

2) Cosa cambia rispetto al CAD oggi vigente?

Ci sarà una firma in più: la "firma elettronica avanzata".

3) In cosa consistono le quattro firme?

a. La "firma elettronica" è un insieme di dati associato ad un altro insieme di dati, utilizzati come metodo di identificazione informatica (si va dalla password alla firma biometrica). Le caratteristiche tecniche non sono definite, né il livello di sicurezza.

b. La "firma elettronica avanzata" è una firma elettronica con alcune caratteristiche di sicurezza (essere connessa in maniera unica al firmatario; essere idonea ad identificare il firmatario; essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati). Può trattarsi, verificati i requisiti, dell' OTP (One Time Password), ad esempio contenuta nella chiavetta utilizzata da alcune banche. Come sia associata la firma elettronica avanzata al firmatario, la definizione non lo precisa.

c. La "firma elettronica qualificata" è la firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma. Nella definizione di firma elettronica qualificata si precisa che l'associazione al firmatario avviene attraverso un certificato qualificato.

d. La "firma digitale" è un particolare tipo di firma elettronica qualificata basata su un sistema di crittografia a chiave pubblica. E' la firma apposta

con smart card o token rilasciato dal certificatore qualificato. In questo caso si sceglie una particolare tecnologia.

4) La definizione di "firma digitale" come "un particolare tipo di firma elettronica avanzata basata su un sistema di chiavi crittografiche" che sarebbe stata introdotta nel Cad era sbagliata?

Sì, perché stando a questa definizione la firma digitale sarebbe stata senza certificato. Stando alle notizie di oggi, risulta modificata la definizione, che tuttavia è ancora priva del riferimento al dispositivo di firma sicuro che invece è ancora presente nella definizione di firma elettronica qualificata. Si potrebbe, semplicemente, non modificare la definizione di firma digitale.

5) In sintesi, quali sono le firme più sicure?

Si confrontano cose diverse.

In sintesi, le definizioni di firma elettronica e di firma elettronica avanzata non si riferiscono a un livello di sicurezza predeterminato o a una tecnologia precisa. Sono "neutre", come previsto dalla direttiva.

Invece, le definizioni di firma elettronica qualificata e digitale, sono collegate a livelli di sicurezza predeterminati e ad una tecnologia predefinita.

6) È corretto affermare che la "firma elettronica avanzata" è imposta dalla direttiva europea e che quella "qualificata" è un'invenzione italiana?

No, non è corretto. Vero è che la direttiva definisce la "firma elettronica avanzata" e non quella "qualificata", ma gli effetti giuridici previsti dalla direttiva si riferiscono a "firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura", cioè alle "firme qualificate".

La "firma elettronica qualificata" è la "firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo per la creazione di una firma sicura" cui la direttiva collega determinati effetti giuridici.

7) Quale efficacia probatoria avranno i documenti con le quattro firme, secondo la bozza di modifica del Cad?

a. Il documento informatico con la firma elettronica sarà, come og-

gi, valutabile dal giudice, caso per caso, sulla base delle caratteristiche di caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

b. I documenti informatici con firma elettronica avanzata, firma elettronica qualificata, firma digitale, avranno la medesima efficacia probatoria, quella prevista dall'art. 2702 del codice civile per la scrittura privata. Come oggi, l'utilizzo del dispositivo di firma si presumerà riconducibile al titolare, salvo che questi dia prova contraria.

8) Saranno gli atti firmati con le quattro firme idonei ad integrare la forma scritta?

a. L'atto con la firma elettronica sarà, come oggi, valutabile dal giudice, caso per caso, sulla base delle caratteristiche di caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

b. Gli atti con firma elettronica avanzata, firma elettronica qualificata, firma digitale potranno integrare la forma scritta.

c. Unica eccezione: la firma elettronica avanzata non basterà per gli atti aventi ad oggetto beni immobili (art. 1350 c.c., nn. 1-12). Solo per questi atti sono richieste la firma elettronica qualificata o la firma digitale.

9) Alcuni esempi?

Le banche potranno utilizzare la firma elettronica avanzata per i contratti bancari. Potrebbero ricondursi alla firma elettronica avanzata (ma occorre verificarne caratteristiche e requisiti) sistemi OTP e firma autografa su dispositivi elettronici.

10)A cosa servirà la firma digitale?

Certamente alla conclusione di contratti aventi ad oggetto beni immobili, alla stipula dell'atto pubblico informatico, alla conservazione sostitutiva".

Capitolo 3

PEC: Aspetti Pratici

3.1 Il documento informatico e l'efficacia probatoria

Utilizzare strumenti informatici e telematici per il traffico giuridico è una realtà: inviare una proposta contrattuale tramite mail, averne lettura e ricevere dalla controparte l'accettazione a stretto giro è divenuto uno strumento di efficienza ormai irrinunciabile, anche in azienda.

Da un punto di vista strettamente giuridico questi semplici passi sono densi di problematiche, di cui si è occupato il legislatore. Un primo problema è quello di considerare il documento informatico non solo come uno strumento utilizzabile per preparare un atto scritto ma, indipendentemente dalla sua traduzione cartacea, come documento in senso stretto.

Superata questa prima impasse, ne sorge un seconda: ricondurre con certezza il documento informatico al suo autore e, successivamente, regolarne il suo valore probatorio.

L'uso della posta elettronica porta con se diverse questioni, più o meno controverse, sulle quali molti giuristi hanno espresso, negli ultimi anni, opinioni discordanti e ad alcune delle quali, solo negli ultimi tempi, il legislatore ha finalmente dato certezza.

La domanda più importante che ci si è posti è quale sia il valore giuridico

della posta elettronica: è giusto considerare un documento alla pari di una e-mail? Se si che valore probatorio ha? È opponibile a terzi?

In via generale l'ordinamento giuridico italiano ha disciplinato diversi aspetti del documento quali la forma, l'efficacia probatoria, la conservazione, la notificazione e la pubblicazione; caratteristica fondamentale del documento deve essere la sua non modificabilità, ed è stato proprio questo aspetto a creare i maggiori problemi per quanto riguarda i documenti su supporto informatico e quindi anche l'e-mail.

Nel modificare un documento cartaceo risulta impossibile non lasciare tracce poiché non è fisicamente possibile scindere il supporto materiale, cioè il foglio di carta, dal suo contenuto, cioè la scrittura[1].[CC05]

Al contrario il documento informatico può essere modificato e i dati possono essere trasferiti, riprodotti e memorizzati su infiniti supporti diversi, facendo risultare impossibile la distinzione tra originale e copia.

Occorre quindi, per avere l'inalterabilità del documento informatico, avvalersi di uno strumento che non sia riferito al supporto ma bensì ai dati in esso contenuti, in modo tale da poterli trasmettere e memorizzare senza però perdere le loro caratteristiche.

Sotto il profilo storico, la prima norma di portata generale che ha introdotto nel nostro ordinamento il principio della validità e della rilevanza giuridica dei documenti informatici è stata l'art.15 comma 2 della legge n. 59/1997.

La norma era inserita all'interno di un intervento dedicato alla semplificazione amministrativa, ma in realtà enunciò un principio destinato ad incidere nell'ambito dei rapporti tra privati (comprese le aziende) e PA.

Nel tempo, la materia è stata oggetto di riordino e complessiva rivisitazione: i vari interventi legislativi sono confluiti nel Codice dell'amministrazione digitale, contenuto nel d.lgs. 7 marzo 2005, n. 82. Secondo la riforma, per

[1] C.Cevenini, C. Di Cocco, G. Sartor, Lezioni di informatica giuridica, 2005 Gedit, Bologna

documento informatico si intendeva la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. p del d.lgs. n. 82/2005).

Nella sua consistenza tradizionale (su supporto cartaceo), il documento assumeva rilevanza sotto due profili: quello della forma degli atti giuridici, e quello della prova.

Per capire come la legge valuta il documento informatico occorre far capo alle diverse tipologie previste dal d.lgs. 23 gennaio 2002. In tal senso, si distinguevano:

- il documento informatico in generale
- quello sottoscritto con firma elettronica
- quello sottoscritto con firma elettronica avanzata (digitale)

Nel primo caso -documento informatico in generale- valeva quanto disposto dall'art. 20 del Codice dell'amministrazione digitale: il documento informatico da chiunque formato (anche dal privato) nonché la registrazione su supporto informatico e la trasmissione con strumenti telematici, risultavano validi e rilevanti a tutti gli effetti di legge. Ciò implicava una generale equiparazione del documento su base informatica al documento su base materiale.

Ulteriore problema era quello dell'appropriazione della scrittura legata alla sottoscrizione. In base alla disciplina passata, non risultava più vero che il documento informatico sottoscritto con firma elettronica soddisfaceva il requisito legale della forma scritta: il legislatore rinunciò ad equiparare il documento sottoscritto con semplice firma elettronica al documento sottoscritto con firma cartacea, ma bensì ricollegò espressamente tale qualificazione soltanto al documento sottoscritto con firma elettronica qualificata o digitale.

Il documento informatico con apposta una firma elettronica, comunque, sul piano probatorio era liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

La firma elettronica semplice, infatti, è data dall'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, lett. q, d.lgs. n. 82/2005). In tal senso, la firma elettronica potrebbe consistere anche in una semplice password o username che siano idonei all'identificazione informatica del firmatario di un documento (si pensi, nell'ambito delle comunicazioni tramite mail, ai dati necessari per collegarsi alla propria casella di posta elettronica ed inviare la relativa comunicazione).

Secondo gli artt. 20, comma 2, e 21, comma 2, del Codice dell'amministrazione digitale, il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfaceva il requisito legale della forma scritta, qualora sia stato formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore e l'integrità del documento.

Nel primo caso -documento informatico in generale- valeva quanto disposto dall'art. 20 del Codice dell'amministrazione digitale: il documento informatico da chiunque formato (anche dal privato) nonché la registrazione su supporto informatico e la trasmissione con strumenti telematici, risultavano validi e rilevanti a tutti gli effetti di legge. Ciò implicava una generale equiparazione del documento su base informatica al documento su base materiale.

Ulteriore problema era quello dell'appropriazione della scrittura legata alla sottoscrizione. In base alla disciplina passata, non risultava più vero che il documento informatico sottoscritto con firma elettronica soddisfaceva il requisito legale della forma scritta: il legislatore rinunciò ad equiparare il documento sottoscritto con semplice firma elettronica al documento sottoscritto con firma cartacea, ma bensì ricollegò espressamente tale qualificazione soltanto al documento sottoscritto con firma elettronica qualificata o digitale.

Il documento informatico con apposta una firma elettronica, comunque, sul piano probatorio era liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

La firma elettronica semplice, infatti, è data dall'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, lett. q, d.lgs. n. 82/2005). In tal senso, la firma elettronica potrebbe consistere anche in una semplice password o username che siano idonei all'identificazione informatica del firmatario di un documento (si pensi, nell'ambito delle comunicazioni tramite mail, ai dati necessari per collegarsi alla propria casella di posta elettronica ed inviare la relativa comunicazione).

Secondo gli artt. 20, comma 2, e 21, comma 2, del Codice dell'amministrazione digitale, il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfaceva il requisito legale della forma scritta, qualora sia stato formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore e l'integrità del documento.

Ne conseguiva che, anche quando la legge richiedesse a pena di nullità la forma scritta (ovvero nei casi un cui il contratto risultava valido solo se redatto per iscritto), il documento sottoscritto con firma elettronica qualificata o con firma digitale soddisfaceva il requisito richiesto.

In tali casi, inoltre, il documento così formato aveva sul piano probatorio l'efficacia prevista dall'art. 2702 del codice civile: la scrittura privata dava piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi la sottoscriveva, se colui contro il quale la scrittura veniva prodotta ne riconosceva la sottoscrizione, ovvero se questa veniva legalmente considerata come riconosciuta.

Dalla lettura della norma si ricava che: il documento informatico dava comunque prova della provenienza delle dichiarazione dal sottoscrittore con firma digitale; se una persona riconosceva la propria firma non poteva disconoscere le dichiarazioni che aveva sottoscritto; il documento informatico si produceva e dava prova contro il sottoscrittore e controparte non poteva portare come prova a proprio favore una dichiarazione formata solo da lui.

A questo punto, il documento informatico poteva essere classificato come tale, secondo l'efficacia probatoria dello stesso.

Nel caso del documento informatico semplice, anche se sottoscritto con firma elettronica semplice, siamo nel campo delle forme libere. Pertanto, l'esistenza di riscontri sullo scambio di messaggi di posta elettronica poteva avere un qualche valore di prova semplice e il documento risultava avere lo stesso valore di prova delle riproduzioni meccaniche o fotografiche, così come espressamente previsto dalla versione dell'art. 2712 del codice civile (le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime).

Diversamente, con la firma elettronica qualificata, ovvero con la firma digitale, il documento informatico assumeva i caratteri e soddisfaceva il requisito legale della forma scritta. Sul piano probatorio, infatti, tale tipologia di documento poteva accedere al grado di forma della scrittura privata autenticata.

Per chiarire quanto detto propongo un esempio: supponiamo che un fornitore di schede video trasmetta tramite posta elettronica ad un proprio cliente un preventivo; questi, ritenuta la proposta conveniente, decide di accettarla ed invia al proprio fornitore una mail nella quale da il benestare al preventivo.

In caso di contratti a distanza, il contratto si perfeziona nel momento in cui l'accettazione giunge a conoscenza del proponente. Pertanto, in caso di revoca della proposta, questa deve giungere al destinatario prima che la sua accettazione sia giunta la proponente. Secondo l'art. 1335 del codice civile, l'accettazione si presume conosciuta nel momento in cui la dichiarazione giunge all'indirizzo del destinatario; tale presunzione è estesa dal d.p.r. n. 513/97 all'indirizzo elettronico (ad esempio alla casella di posta elettronica).

Se la fornitura viene eseguito *nulla questio*, ma se il fornitore/cliente non adempie ai suoi obblighi o sorgono questioni sull'interpretazione del contratto, occorre affrontare il valore probatorio delle comunicazioni intercorse.

In questo senso, se il documento informatico è sottoscritto con firma di-

gitale esso è equiparato in tutto e per tutto al documento cartaceo firmato. Diversamente, il giudice valuterà liberamente le comunicazioni intercorse tra le parti.

Per l'analisi del documento informatico e del suo valore probatorio all'interno del CAD 2010, riporto un interessante articolo tratto dal Blog della professoressa Giusella Finocchiaro[2][urle]: "Il file privo di ogni tipo di firma è probabilmente il documento informatico più diffuso. Esso ha una specifica efficacia probatoria, già riconosciuta dalla legge e anche dalla giurisprudenza, addirittura di Cassazione (Cass. 11445/2001; Cass. 9884/2005).

Sull'efficacia probatoria di questa tipologia di documento informatico non c'è mai stato grande dibattito, ma anzi c'è sempre stato un sostanziale accordo fra dottrina, legislatore e giurisprudenza.

L'efficacia del documento informatico, che si affermava ai sensi dell'art. 2712 del codice civile, richiamato dall'art. 23 del previgente CAD, è quella delle riproduzioni meccaniche, le quali formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti e alle cose medesime.

Apparentemente il nuovo art. 23-quater del Codice dell'amministrazione digitale, sembra confermare la norma previgente, disponendo: all'art. 2712 del codice civile dopo le parole: "riproduzioni fotografiche" è inserita la seguente: , "informatiche", esattamente come già disponeva l'art. 23 del CAD previgente.

Invece, nel nuovo art. 20, comma 1-bis, si legge: "L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'art. 21".

Quindi ci sono due norme nel nuovo CAD che disciplinano la stessa fattispecie: l'efficacia probatoria del documento informatico senza firma.

Quale applicare?

[2]http://www.blogstudiolegalefinocchiaro.it/tag/efficacia-probatoria/

Non potendo due norme diverse (nuovo art. 20, comma 1-bis e nuovo art. 23-quater) disciplinare in modo diverso l'efficacia probatoria della medesima fattispecie (il documento informatico senza firma), non resta che sperare in un intervento correttivo del legislatore."

Lo scenario che si presenta, dunque, è tuttora quello di una imprecisa applicazione delle norme, il che porta ad un auspicabile intervento da parte del legislatore, quantomeno per arginare la duplice esistenza di queste riguardo il medesimo ambito, ma, più nello specifico, anche per valorizzarne l'efficacia e la valenza.

All'interno del vigente CAD inoltre, si elencano le qualità che un documento deve possedere affinché venga riconosciuta la sua efficacia probatoria; queste rispondono al nome di qualità, sicurezza, integrità ed immodificabilità: attributi che nell'informatica possono essere raggiunti solo e soltanto con adeguate ed attente procedure tecniche.

Inoltre viene specificato, articoli 14-2- 2bis[3], che il documento informatico, se provvisto di alcune tipologie di firme elettroniche, può avere l'efficacia prevista dall'articolo 2702 e 1350 del c.c. . Si noti anche la presenza di una differenza tra un documento sottoscritto con firma elettronica avanzata e firma elettronica qualificata e quindi firma digitale. In realtà la validità della firma elettronica avanzata è stata inserita perchè presente nelle direttive europee.

Ancora, sul documento informatico c'è da soffermarsi particolarmente sull'articolo 15, in merito alle copie informatiche di documenti analogici;l'articolo 15 è un articolo molto importante per i processi di conservazione sostitutiva, perchè modifica l'articolo 22 del vecchio CAD. L'art. 22 afferma che un documento informatico, "nato" da una copia di un documento analogico, per avere l'efficacia degli articoli 2714 e 2715 del codice civile, deve avere obbligatoriamente la firma digitale o altra firma elettronica qualificata, anche senza l'intervento di un pubblico ufficiale (per i privati il notaio), poiché in questo caso si tratta di un documento analogico non unico. Diversamente

[3]Www.digitpa.gov.it

nel comma 2 è richiesto per forza di cose l'intervento del pubblico ufficiale, poiché trattasi di documenti analogici unici. Ma il comma 2 non dice solo questo. Infatti a leggere attentamente, si parla di "copie per immagine" (come si legge anche nel comma 3), quindi affinché un documento informatico possa sostituire un documento analogico, può essere solo e soltanto scansionato. Sarebbe stato meglio se, visto comunque la presenza del notaio, fosse stato ammissibile avere una copia informatica del contenuto di un documento analogico e non anche obbligatoriamente della forma di quest'ultimo. Il comma 4 dice semplicemente che con i documenti informatici possono essere assolti gli obblighi di conservazione, ma solo se vengono rispettati i comma 1,2 e 3. I commi 5 e 6 , invece, indicano che esiste una particolare tipologia documentale analogica (penso ad esempio agli archivi storici o quelli delle PA) che al momento non potrebbero essere dematerializzati, o comunque nel caso fossero dematerializzati, permane l'obbligo per questa tipologia documentale dell'intervento del notaio nei processi di conservazione sostitutiva. Per quel che riguarda, se cosi si può dire, il processo inverso, ovvero le copie analogiche di documenti informatici, si deve far fede all'articolo 16, che disciplina quest'aspetto, in breve, l'articolo 16 che modifica l'articolo 23 del vecchio CAD, afferma che un documento informatico può essere trasformato in un documento analogico, con lo stesso valore probatorio, solo se la copia analogica è attestata da un pubblico ufficiale. Questa considerazione deriva dal semplice fatto che quando si effettua la stampa di un documento nativo informatico con oltretutto apposta una firma digitale, tale stampa perde ovviamente le proprietà di integrità, immodificabilità, sicurezza e qualità. Come ben si può comprendere la firma digitale esiste solo e soltanto in un ambiente informatico e non certo su un supporto analogico. Inoltre l'articolo 16 richiama ancora una volta la figura del notaio anche nel caso in cui si effettui una copia informatica di un altro documento informatico originale, ma che abbia un'impronta diversa rispetto proprio a quella dell'originale. Quindi se l'hash di una copia di un documento informatico varia, allora essa non è conforme all'originale o, per usare un termine legislativo, non viene

riconosciuto come duplicato. Una considerazione da fare molto importante è sul comma 5, riferito ai documenti amministrativi informatici. Tale comma infatti, permette in fase di stampa di un documento informatico, il riconoscimento del cosiddetto timbro digitale. Tale timbro digitale infatti, risolve in maniera sicura e certa, il problema di copia analogica di un documento informatico con firma digitale. Infatti con un contrassegno elettronico, sarà sempre possibile risalire all'unico documento informati originale.

Dopo l'analisi dell'efficacia probatoria di un documento informatico, attraverso l'evoluzione che ha avuto all'interno dei CAD dal 2005 ad oggi, spostiamo ora l'attenzione sull'uso della firma digitale e della firma elettronica all'interno della posta elettronica certificata.

3.2 Firma elettronica e firma digitale nella PEC

Alla luce di quanto finora detto, si può delineare una linea che differenzi i due principali strumenti fino ad ora analizzati: la PEC e la firma digitale.

La PEC è uno strumento che viene utilizzato per l'invio di documenti che va a sostituire i mezzi tradizionali quali, ad esempio, la raccomandata A/R, il fax oppure il corriere. La firma digitale invece, dal canto suo, rappresenta il mezzo elettronico per apporre la propria firma ad un documento elettronico o ad una mail. In altri termini, la firma digitale è il sostituto elettronico della firma autografa in calce ai documenti cartacei.

La PEC è uno strumento che assicura che un messaggio arrivi a destinazione inalterato e integro e garantisce l'identità del mittente; con la firma digitale invece, il mittente appone il proprio autografo al contenuto della mail ed agli eventuali allegati, come ulteriore garanzia della propria identità.

Si intende che i due strumenti non sono in contrapposizione, ma possono essere utilizzati insieme.

Per il funzionamento della PEC non è necessario nessun tipo di device, mentre per l'utilizzo della firma digitale è necessario dotarsi di un letto-

re di smart card o di un token USB, solitamente di facile reperimento in commercio.

In definitiva, si può affermare che l'utilizzo combinato di PEC e firma digitale diano un livello di sicurezza elevato per quel che riguarda la trasmissione sicura di un documento: analizziamo brevemente il motivo.

Il solo invio di documenti tramite posta elettronica certificata fornisce si, come detto finora, un valido strumento per l'identificazione del mittente, ma tuttavia ci si può trovare difronte a un caso di invio improprio. Nel momento in cui un account di posta elettronica venga lasciato aperto, può succedere che chiunque abbia accesso a quella macchina abbia la possibilità di inviare materiale, che di fatto risulterebbe a nome del titolare della casella, ma che nella realtà non corrisponde al vero.

In questo caso, se l'invio del documento risulta accompagnato invece da firma digitale apposta, prova realmente l'identità del mittente, poiché per l'apposizione di firma si necessita di ulteriore conoscenza di informazioni, quali user-id e password.

Nel momento in cui ci si trova difronte a invio improprio anche in caso di apposizione di firma digitale su un documento inviato tramite PEC si va incontro a sanzioni legali di altro genere, riguardanti phising o furti d'identità di cui si accennerà più avanti in questo lavoro.

Resta in ogni modo certo il fatto che, in nessun modo sia collegato l'uso di caselle di posta elettronica certificata all'uso di firma digitale.

Come prova ulteriore di quanto scritto, riporto un interessante articolo pubblicato da M. Salzano in merito alla PEC e alla firma digitale[4][urlf]: "Quali garanzie dà la firma digitale dell'utente applicata ad un messaggio di posta elettronica o ad un allegato?La firma digitale posta dall'utente garantisce:1) la provenienza; il certificato usato per la firma è associato univocamente ad una persona fisica; 2)l'integrità; se il destinatario verifica che la firma è corretta è sicuro che nessuno ha alterato il documento dopo l'apposizione della firma. Ci sono due tipi di firme utilizzabili:

[4]Www.fnada.it

- La firma del messaggio, apposta con certificato di autenticazione; può essere verificata dai principali strumenti utilizzati per la consultazione della posta elettronica. E' importante che il certificato contenga il nome della casella utilizzata per l'invio, altrimenti alcuni strumenti segnalano un problema di coerenza nella firma.

- La firma di sottoscrizione a norme AIPA, apposta su un documento allegato ad un messaggio; questa fornisce la garanzia più completa dal punto di vista legale. La verifica della firma va effettuata con lo strumento fornito dall'autorità di certificazione che lo ha emesso.E' possibile utilizzare congiuntamente le due firme. E' importante, in fase di verifica della firma, controllare anche le liste di revoca dei certificati."

La posta elettronica certificata, in connubio con la firma digitale, può però portare ad un altro tipo di problemi, legato al flusso documentale.

Fin dalla nascita la PEC ha destato molti dubbi e sollevato parecchie perplessità, in questo caso si potrebbe avere uno sconvolgimento informatico, dovuto alla sottoscrizione elettronica, ovvero la firma elettronica non qualificata.

Si deve notare che lo sconvolgimento di cui sopra si parla potrebbe nono esserci nel momento in cui:

1. la firma digitale rimane, nell'ambito della gestione informatica dei flussi documentali, il superiore contrassegno di autenticità, per nulla scalfito dalla configurazione della PEC come firma elettronica (non qualificata). Nella disciplina generale della trasmissione telematica alle pubbliche amministrazioni di istanze e dichiarazioni, ci si affida alla firma digitale quale strumento che può essere configurato come indispensabile nei casi necessari: è fatto noto che le pubbliche amministrazioni possano stabilire quando è necessaria la sottoscrizione con firma digitale. Le cautele di una corretta gestione dei flussi documentali, anzi, impongono alle pubbliche amministrazioni di effettuare tale valutazione ai fini della conseguente scelta: si configura, quindi, una deroga al generale

principio di possibilità di utilizzo della sola PEC (o della carta nazionale servizi o, ancora, della carta d'identità elettronica). La predetta disposizione è ribadita dalla norma secondo cui le pubbliche amministrazioni devono sì accettare l'invio, da parte dei cittadini, di istanze tramite PEC (o CEC-PAC), ma non per questo esse sono private del potere di richiedere anche la sottoscrizione con firma digitale (ove lo ritengano, appunto, necessario.

2. L'invio di un'istanza tramite PEC (senza firma digitale ove non escluso dall'amministrazione destinataria) sarà inquadrato, dal ricevente/gestore del flusso documentale, come firma elettronica non qualificata, la cui efficacia probatoria deriverà dalle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. La configurabilità della PEC come firma elettronica (non qualificata) costituisce un riflesso della peculiare gerarchia italiana delle firme elettroniche: d'altro canto, nel recente passato in molti propugnarono la tesi della configurabilità della semplice e-mail come firma elettronica "leggera"; coerentemente, adesso non si dovrebbe pretendere di spogliare la PEC del requisito reclamato con vigore, invece, per il suo parente "povero".

3. La PEC, nell'ambito della gestione dei flussi documentali di una pubblica amministrazione, non deve essere isolata dal procedimento amministrativo di riferimento: la PEC può essere uno strumento prezioso per lo stesso procedimento, se sottoposta a corrette e predeterminate regole di gestione, in armonia con la disciplina dell'iter del procedimento amministrativo; la PEC, se proficuamente integrata nel protocollo informatico, può apportare un benefico arricchimento delle informazioni sui flussi documentali.

4. Un buon sistema di protocollo informatico e di gestione dei flussi documentali dovrebbe già da tempo aver consolidato regole di trattamento della PEC; la configurazione della PEC quale firma elettronica non qualificata sarà disciplinata, ove non già previsto nel manuale di gestione,

con un opportuno adeguamento dello stesso manuale, finalizzato ad armonizzare le procedure relative ai documenti con firma elettronica non qualificata, con le eccezioni di trattamento sopra previste (che dovranno essere trasparenti, come impone la normativa sul protocollo informatico).

Il problema dunque non dovrebbe essere legato alla configurazione della PEC quale firma elettronica, ma la gestione informatica dei flussi documentali potrebbe subire qualche ripercussione qualora tra i cittadini si diffonderà intensamente l'uso della PEC gratuita per dialogare con le pubbliche amministrazioni: queste ultime, infatti, si potrebbero trovare impreparate a gestire un'improvvisa massa di comunicazioni telematiche (si aggiungeranno le comunicazioni inviate tramite PEC da professionisti e imprese).

E' possibile, in effetti, che gli utenti, una volta acquisita confidenza con il nuovo strumento e scoperta l'economicità di PEC e CEC-PAC rispetto alla raccomandata A/R, inizieranno a sommergere le pubbliche amministrazioni di comunicazioni ridondanti e superflue: questo è uno dei rischi che dovrà essere affrontato con una accorta gestione dei flussi documentali.

In ogni modo, come per il documento informatico nei paragrafi precedenti, andremo ora ad analizzare il valore giuridico delle e-mail, analizzando vari casi.

3.3 Il valore giuridico delle e-mail

Anche per questa parte di lavoro partirò con l'analizzare i casi principali del passato, nati con il CAD 2005, per poter vedere le evoluzioni e le casistiche che ci hanno portato fino ai giorni nostri.

Non c'è alcun dubbio sul fatto che l'e-mail è a tutti gli effetti un documento informatico visto che costituisce una rappresentazione informatica di documenti, immagini, video e di ogni altro elemento che possa essere giuridicamente rilevante. Il punto fondamentale è capire se l'e-mail ha il valore di un

documento informatico non sottoscritto oppure di un documento informatico sottoscritto con firma elettronica almeno leggera.

Per stabilire quale fosse l'effettivo valore giuridico della posta elettronica bisognava partire con il distinguere il diverso valore attribuibile alla categoria del documento informatico, che in base all'articolo 1 del d.lgs. n.82/2005, era "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" , categoria alla quale apparteneva certamente anche l'e-mail nel momento in cui si rappresentavano al suo interno atti fatti o dati giuridicamente rilevanti[5].[Jor05]

In base all'articolo 20, comma 1 del Codice dell'Amministrazione Digitale si leggeva 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 qualora siano conformi alle disposizioni del suddetto codice e alle regole tecniche di cui all'articolo 71"; il comma 2 inoltre specificava che il requisito legale della forma scritta veniva soddisfatto esclusivamente dal documento informatico sottoscritto con firma elettronica qualificata o con firma digitale "se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71[6] che garantivano l'identificabilità dell'autore e l'integrità del documento".

L'articolo 21 invece, definiva il diverso valore probatorio attribuibile al documento informatico in base al tipo di sottoscrizione che lo accompagnava; il documento informatico a cui era apposta una firma elettronica era liberamente valutabile dal giudice tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

Il legislatore dunque, non attribuiva al documento informatico con firma elettronica una determinata efficacia probatoria poiché non faceva riferimento

[5]Si legga in proposito, M. G. Jori, l'efficacia probatoria dell'e-mail, in Giurisprudenza Italiana, n. 5, 2005

[6]L'articolo 71 disponeva che le regole tecniche venissero emanate con i decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'Innovazione e le Tecnologie e che le regole tecniche nelle materie del codice dovevano restare in vigore sino all'adozione di quelle nuove.

ne all'art. 2712 c.c. per le riproduzioni meccaniche, ne all'art. 2702 c.c., sull'efficacia della scrittura privata riconosciuta, ma richiamava il più generale principio della libera valutazione delle prove da parte del giudice.

Viceversa il documento informatico con firma digitale o firma elettronica qualificata dava piena prova fino a querela di falso della provenienza delle dichiarazioni di chi lo sottoscriveva. Aveva quindi l'efficacia probatoria della scrittura privata riconosciuta e l'utilizzo del dispositivo di firma si presumeva riconducibile al titolare, salvo che fosse data prova contraria.

Il comma 3 del suddetto articolo precisava, inoltre, che "l'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basta su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate".

Le disposizioni cosi espresse valevano sia che il certificato fosse stato emesso da un certificatore stabilito in uno Stato membro dell'Unione

Europea, sia nel caso in cui il certificatore sia extraeuropeo purchè questi fosse in possesso dei requisiti stabiliti dalla direttiva 1999/93 CE e fosse accreditato presso uno stato membro oppure il certificato qualificato fosse garantito da un certificatore stabilito dall'Unione, oppure il certificato qualificato o il certificatore fossero riconosciuti in base ad accordi bilaterali o multilaterali tra l'Unione e Paesi Terzi o organizzazioni internazionali.

L'art. 23 inseriva all'art. 2712 c.c., dopo le parole "riproduzioni fotografiche", la parola "informatiche" in modo tale che anche le copie informatiche formassero piena prova dei fatti e delle cose rappresentate, se colui contro il quale erano prodotte non ne disconoscevano la conformità ai fatti o alle cose medesime.

Nel caso della posta elettronica, essa va considerata come un semplice documento informatico equivalente ad una riproduzione meccanica oppure ad un documento informatico sottoscritto con firma elettronica semplice e

quindi che soddisfaceva il requisito della forma scritta ex art. 20 del d.lgs. n.82/2005.

L'argomento è stato al centro di un ampio dibattito dottrinale; la causa scatenante era da rilevarsi nella pubblicazione dei decreti ingiuntivi del Tribunale di Cuneo[7] e del Tribunale di Mondovì[8] nei quali fu dedotto un riconoscimento di debito sulla base della sola produzione di uno scambio di e-mail.

Tali pronunce furono poi seguite da altre sempre sulla stessa linea.

Il Giudice sostenne, quindi, la tesi secondo la quale l'e-mail era equipollente a un documento scritto in base al fatto che un nome utente e una password potessero in qualche modo rappresentare una forma di autenticazione informatica e, quindi, costituire una firma elettronica semplice[9][Lis04].

Molti giuristi però, obbiettarono al riguardo, che non fosse assolutamente vero che nome utente e password costituissero una firma elettronica semplice, poiché non rispondeva ai requisiti previsti dall'art.1 del d.lgsl. n. 10/2002[10], che, come già detto, definiva la firma elettronica come "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"; infatti nome utente e password sono, tuttora, certamente dati in forma elettronica, ma la loro immissione nella fase iniziale di accesso al server non comporta, e non comportava, però, alcuna associazione logica tra questi dati e gli altri dati elettronici che costituiscono il messaggio e-mail.

Perciò sul piano del diritto non vi è stato alcun elemento per affermare che l'accesso con nome utente e password al servizio e-mail potesse configurare la firma elettronica dei documenti inviati e sul piano del fatto era fin troppo facile far apparire un identità fittizia come mittente delle e-mail. Molti di quelli che ritennero che dalle norme si potesse evincere la natura di firma

[7]Si veda il decreto ingiuntivo n.848 del 15 dicembre 2003

[8]Si veda il decreto ingiuntivo n.375 del 7 giugno 2004

[9]Si legga a riguardo A.Lisi, l'e-mail è "forma scritta"?, in www.altalex.com , 2004

[10]I requisiti previsti dall'art.1 del d.lgsl. n.10/2002 per la firma elettronica furono poi ripresi dall'articolo 1 del Codice dell'Amministrazione Digitale

elettronica per nome utente e password , finirono col chiedersi se le stesse norme non fossero sbagliate[11].[MC04]

Quindi, per concludere, se il valore comune della semplice e-mail è quello di documento informatico sottoscritto con firma elettronica leggera, l'e-mail in un qualsiasi giudizio soddisfaceva il requisito della forma scritta e poteva essere fatta valere come prova, ma se la parte contro cui veniva prodotta la disconosceva, essa poteva essere liberamente valutabile dal giudice a seconda di quanto gli sembrava certo che l'e-mail provenisse effettivamente dal soggetto da cui risultava inviata.

Ovviamente se si voleva garantire un maggior valore, sia dal punto di vista sostanziale che probatorio, alla propria mail, conveniva attrezzarsi per sottoscriverla con una firma elettronica avanzata o, meglio ancora, con firma elettronica qualificata.

Il Consiglio dei Ministri, su proposta del ministro per le innovazioni e le tecnologie Lucio Stanca, emanò un DPR che attribuiva valore legale alle e-mail certificate, equiparando la posta elettronica alle raccomandate, sia nei rapporti con la pubblica amministrazione che tra privati.

Se da un lato apparve essere un simbolo di progresso, dall'altro presentava alcuni limiti e titubanze da tenere in considerazione.

Ancora non chiara risultava la posizione delle e-mail semplici, se possedevano o meno valore legale. Vi era chi lo negava fermamente e chi, invece, rimetteva la decisione alla discrezionalità del giudice, da esaminarsi caso per caso. Una logica associazione fa sostenere ad alcuni che se la e-mail certificata aveva valore di raccomandata A/R, quanto meno la e-mail semplice avrebbe avuto valore di posta prioritaria.

Famosi sono stati i decreti ingiuntivi emessi dal Tribunale di Cuneo e di Bari sulla base della produzione di e-mail contenenti il riconoscimento di un debito.

Il legislatore italiano stava tentando di rivoluzionare la nostra "forma

[11]Si legga a riguardo, M. Cammarata, E. Maccarone, un messaggio è-mail non è "prova scritta", in www.interlex.it, 2004

mentis", abituata allo scritto cartaceo, instradando la corrispondenza verso il mondo telematico che stava ormai, occupando un ruolo centrale nello scambio di informazioni, che non poteva continuare ad essere formalmente ignorato.

Evidente apparve come il decreto Stanca, così innovativo, abbia in parte mancato di dare spiegazioni ai problemi e alle questioni sopra evidenziate. Non si devono perdonare le lacune legislative, ritenute inevitabili per affrontare e disciplinare un discorso delicato come il valore legale da attribuire alla posta elettronica, ma bisognava incentrarsi sul fatto che, con il tempo, il contenuto del decreto potesse pienamente amalgamarsi alle esigenze degli utenti, arrivando a semplificare ed economicizzare il mondo della corrispondenza.

Passiamo dunque ad analizzare la situazione nell'attuale codice dell'amministrazione digitale.

All'interno di questo codice abbiamo già parlato dell'introduzione della posta elettronica certificata (PEC) e di quale valore gli si voglia attribuire.

Dal 25 gennaio 2011 sono entrare in vigore le ultime novità sulla posta elettronica certificata, dove diventa ufficiale la completa equiparazione tra atto notificato via posta ordinaria o PEC (trasmissione del documento informatico). Tutto ciò è previsto dopo le modifiche introdotte dal decreto legislativo 235/2010.

Tutto ciò può comportare un enorme vantaggio, per esempio, per gli studi professionali che potranno rendere effettive azioni legali, ricorsi o impugnazioni inviando l'atto di controparte tramite casella di posta certificata, a tutto vantaggio di costi e tempistiche. La casella PEC, infatti, è capace di attestare legalmente l'avvenuta ricezione in termini di data e ora di trasmissione, tra l'altro opponibili ai terzi se realizzate secondo le disposizioni del Dpr 68/2005.

Atti, documenti e fatture possono quindi essere inviati telematicamente preservando la propria rilevanza processuale e il valore legale e giuridico, in tutto e per tutto pari a quelli riconosciuti se trasmessi a mezzo raccomandata o tramite ufficiale giudiziario. Dal punto di vista della ricezione della posta certificata, i benefici consistono nella possibilità di mettere in atto la

conservazione sostitutiva, risparmiando ancora una volta tempo e costi legati alla gestione e al reperimento delle informazioni.

Vantaggi che si possono sfruttare per realizzare, ad esempio, un processo gestionale interno di conservazione a norma dei documenti che, se certificato da un conservatore accreditato presso DigitPa (articoli 44 e 44-bis del nuovo CAD) garantiranno una maggiore valenza probatoria per quelli conservati.

Sempre in materia di valenza probatoria, l'art. 6 del CAD è stato integralmente riscritto, al fine di allinearne il contenuto alle modifiche che, di volta in volta, ne hanno ritoccato il testo fino quasi a renderlo una rappresentazione stratificata delle volontà del legislatore succedutesi nel tempo.

Viene ulteriormente rafforzato l'obbligo per le pubbliche amministrazioni di utilizzare la posta elettronica certificata per tutte le comunicazioni in cui sia necessaria una ricevuta di invio e una di consegna con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.

La comunicazione alla PA del proprio indirizzo di posta elettronica certificata comporta, infatti, due ordini di conseguenze:

- in primo luogo, essa costituisce espressa accettazione del dichiarante dell'invio degli atti e documenti che lo riguardano da parte dell'amministrazione;

- in secondo luogo, comporta un vincolo, solo per il soggetto, a ricevere tali atti di cui è necessaria la conferma di avvenuta consegna e ricezione presso quella casella di posta.

Inoltre, al fine di razionalizzare e uniformare il sistema di consultazione degli indirizzi di posta elettronica, viene disposta l'emanazione di un apposito regolamento a cura di DigitPA, sentito il Garante Privacy.

Anche le modifiche dell'art. 48 del CAD hanno lo scopo di allineare il CAD su vari aspetti della posta elettronica certificata regolati successivamente al 2005 in altri atti normativi e regolamentari.

L'unica vera novità è l'equiparazione dell'invio tramite PEC alla Notificazione per mezzo della posta "salvo che la legge disponga diversamente" e non più nei soli casi previsti dalla legge.

Infine, con la modifica dell'art. 65 del CAD si riconosce la Posta Elettronica Certificata come valido sistema di presentazione telematica di istanze e dichiarazioni alla PA: le istanze saranno valide, però, solo ove le credenziali di accesso alle PEC siano state rilasciate previa identificazione del titolare e ciò sia attestato dal Gestore di PEC nel corpo del messaggio o in un apposito allegato.

La precedente formulazione della lett. c-bis), del comma 1 dell'art. 65 del CAD, invece, faceva riferimento alle sole istanze inviate tramite la posta elettronica certificata rilasciati gratuitamente dalla PA ai cittadini ai sensi dell'art. 16 della Legge 2/2009 (la cosiddetta CECPAC).

Appare evidente come la normativa non regoli ancora del tutto bene lo scenario di chi riceve comunicazioni attraverso posta elettronica certificata; finora non si è data molta importanza al fatto che un utente l'abbia letto o meno un messaggio, oppure se avesse la macchina su cui riceve posta in riparazione, oppure se ha smarrito le credenziali d'accesso o non ha scaricato per tempo la posta.

Di fronte la legge la posta risulta consegnata, quindi bisogna prestare anche molta attenzione nel consegnare il proprio indirizzo di posta elettronica certificata.

Nuovo compito del legislatore sarà regolamentare anche questi aspetti della disciplina.

Dopo aver parlato del valore giuridico della PEC, passiamo ora a studiarne un po' più nello specifico l'evoluzione normativa, partendo dal d.p.r n.68/2005 per arrivare ai giorni nostri, ovvero il d.p.r. 235/2010.

3.4 PEC: dal d.p.r. n.68/2005 al 235/2010

Come abbiamo già detto in precedenza, la trasmissione telematica dei documenti informatici costituisce una tematica di notevole interesse perché costituente la base giuridica per un uso "quotidiano" degli strumenti offerti dalla diffusione di Internet (primo fra tutti, la posta elettronica), tanto nei rapporti tra soggetti privati quanto nell'agire della Pubblica Amministrazione.

Sotto il profilo normativo, occorre ricordare che già il D.p.r. 513/1997 (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[12] prevedeva una specifica disposizione rubricata trasmissione del documento con la quale si stabiliva che il documento informatico si intendeva inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di trasmissione o ricezione, inoltre, se conformi a regole tecniche da emanarsi, sarebbero stati opponibili ai terzi.

Le medesime regole tecniche avrebbero dovuto altresì individuare modalità di trasmissione in grado di assicurare l'avvenuta consegna, cosicché ciò sarebbe potuto equivalere alla notificazione a mezzo posta[13].

[12] Gli atti, dati e 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 strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare, entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2 della legge 23 agosto 1988 n. 400. Gi schemi dei regolamenti sono trasmessi alla Camera dei Deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni.

[13] Si segnala, tuttavia, come le regole tecniche in questione, tanto nella loro stesura del 1999 che in quella del 2004, pur recando "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici", in realtà della trasmissione del documento non parlano. Si dovrà attendere il 2005 per una compiuta regolamentazione del fenomeno della trasmissione del

La norma venne poi trasfusa nel T.U.D.A. 445/2000 (art. 14) nello stesso identico testo, per essere modificata nel solo comma 1 dal D.p.r. 68/2005, all'articolo 3[14], ed essere ripresa, in modo identico, nell'articolo 45, comma II del Codice dell'Amministrazione Digitale (D.lgs 82/2005).

Rispetto all'originaria formulazione si palesata la volontà di dare rilevanza giuridica alle due fasi, invio e consegna, del viaggio telematico della posta elettronica: non più un'unica presunzione di conoscibilità che si formava quando il messaggio veniva trasmesso all'indirizzo elettronico dichiarato dal destinatario, ma due presunzioni (una per l'invio, l'altra per la consegna), che si formavano rispettivamente quando il messaggio elettronico veniva trasmesso al proprio gestore e quando risultava disponibile all'indirizzo di posta elettronica del destinatario.

E' bene ricordare a tal proposito che, in base all'art. 2 del Codice dell'Amministrazione Digitale, le norme relative alla trasmissione di documenti informatici si applicano anche ai privati, di conseguenza la regola appena enunciata è da allora divenuto il principio diretto a governare il momento di conclusione di accordi tra soggetti in ambiente telematico.

Con D.M. 2 novembre 2005 (pubblicato in G.U. 15 novembre 2005, n. 266) sono state dettate le regole tecniche di funzionamento della Posta Elettronica Certificata che, come vedremo, disegnano un sistema chiuso basato sul principio del c.d. "dialogo sicuro": al fine di poter garantire la completa tracciabilità del flusso dei messaggi questi non devono transitare su sistemi esterni al circuito di posta certificata.

La porta d'ingresso al mondo della posta certificata è rappresentata dal c.d. punto d'accesso, ovverosia (secondo la definizione contenuta nell'allega-

documento informatico nel nostro ordinamento.

[14]Articolo 3 - Trasmissione del documento informatico Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e' sostituito dal seguente: 1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

to delle richiamate regole tecniche) "il punto che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione, di imbustamento del messaggio originale nella busta di trasporto".

La possibilità da parte di un utente di accedere ai servizi di PEC tramite il punto di accesso deve prevedere necessariamente l'autenticazione al sistema da parte dell'utente stesso. Le modalità di autenticazione possono prevedere, ad esempio, l'utilizzo di user-id e password o, se disponibili e ritenute modalità necessarie per il livello di servizio erogato, la carta d'identità elettronica o la carta nazionale dei servizi. La scelta della modalità con la quale realizzare l'autenticazione è lasciata al gestore. L'autenticazione è necessaria per garantire che il messaggio sia inviato da un utente del servizio di posta certificata i cui dati di identificazione siano congruenti con il mittente specificato, al fine di evitare la falsificazione di quest'ultimo.

Una volta autenticatosi al punto di accesso, l'utente è in grado di spedire un messaggio di posta elettronica certificata con le medesime modalità di redazione ed invio di un messaggio di posta elettronica semplice.

La diversità, infatti, non viene colta in questa fase poiché si realizza unicamente lato gestore, in un processo rispetto al quale l'utente rimane sostanzialmente estraneo. Il messaggio di posta, infatti, viene inserito in una struttura S/MIME (la c.d. busta di trasporto), firmata con la chiave privata del gestore di posta certificata. Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header (intestazione) specifico, consentendo così di garantirne l'univocità nel complesso dell'infrastruttura.

Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale operando una serie di controlli tra cui, ad esempio, il fatto che non siano presenti indirizzi dei destinatari del messaggio nel campo CCN (la PEC non consente infatti l'invio c.d. in copia conoscen-

za nascosta): qualora il messaggio non superi i predetti controlli, esso non potrà essere accettato dal punto di accesso il quale genererà l'avviso di non accettazione.

In caso contrario, verrà prodotta la ricevuta di accettazione, costituita da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.

E' bene ricordare a tal proposito che, in base all'art. 2 del Codice dell'Amministrazione Digitale, le norme relative alla trasmissione di documenti informatici si applicano anche ai privati, di conseguenza la regola appena enunciata è da allora divenuto il principio diretto a governare il momento di conclusione di accordi tra soggetti in ambiente telematico. Con D.M. 2 novembre 2005 (pubblicato in G.U. 15 novembre 2005, n. 266) sono state dettate le regole tecniche di funzionamento della Posta Elettronica Certificata che, come vedremo, disegnano un sistema chiuso basato sul principio del c.d. "dialogo sicuro": al fine di poter garantire la completa tracciabilità del flusso dei messaggi questi non devono transitare su sistemi esterni al circuito di posta certificata. La porta d'ingresso al mondo della posta certificata è rappresentata dal c.d. punto d'accesso, ovverosia (secondo la definizione contenuta nell'allegato delle richiamate regole tecniche) "il punto che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione, di imbustamento del messaggio originale nella busta di trasporto". La possibilità da parte di un utente di accedere ai servizi di PEC tramite il punto di accesso deve prevedere necessariamente l'autenticazione al sistema da parte dell'utente stesso. Le modalità di autenticazione possono prevedere, ad esempio, l'utilizzo di user-id e password o, se disponibili e ritenute modalità necessarie per il livello di servizio erogato, la carta d'identità elettronica o la carta nazionale dei servizi. La scelta della modalità con la quale realizzare l'autenticazione è lasciata al gestore. L'autenticazione è necessaria per garantire che il messaggio sia inviato da un utente del servizio

di posta certificata i cui dati di identificazione siano congruenti con il mittente specificato, al fine di evitare la falsificazione di quest'ultimo. Una volta autenticatosi al punto di accesso, l'utente è in grado di spedire un messaggio di posta elettronica certificata con le medesime modalità di redazione ed invio di un messaggio di posta elettronica semplice. La diversità, infatti, non viene colta in questa fase poiché si realizza unicamente lato gestore, in un processo rispetto al quale l'utente rimane sostanzialmente estraneo. Il messaggio di posta, infatti, viene inserito in una struttura S/MIME (la c.d. busta di trasporto), firmata con la chiave privata del gestore di posta certificata. Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header (intestazione) specifico, consentendo così di garantirne l'univocità nel complesso dell'infrastruttura. Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale operando una serie di controlli tra cui, ad esempio, il fatto che non siano presenti indirizzi dei destinatari del messaggio nel campo CCN (la PEC non consente infatti l'invio c.d. in copia conoscenza nascosta): qualora il messaggio non superi i predetti controlli, esso non potrà essere accettato dal punto di accesso il quale genererà l'avviso di non accettazione. In caso contrario, verrà prodotta la ricevuta di accettazione, costituita da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.

La ricevuta di accettazione è una delle due ricevute che il titolare di una casella di posta elettronica certificata vede recapitarsi quando invia un messaggio ad un altro indirizzo PEC.

La seconda ricevuta, giuridicamente più importante e che costituisce l'alternativa digitale alla tradizionale ricevuta di ritorno della raccomandata cartacea, è quella di avvenuta consegna che può essere di tre tipi, a seconda della scelta effettuata dall'utente al momento dell'invio del messaggio.

La prima tipologia è quella completa: la ricevuta comprende non soltanto i dati del mittente e del destinatario, l'oggetto, la data e l'ora di avvenuta consegna, ma anche il contenuto del messaggio originario, comprensivo di

allegati. La ricevuta completa è generata per ciascuno degli indirizzi di destinazione (l'utente avrà tante ricevute quanti sono gli indirizzi indicati nel campo "TO"), fatta eccezioni per quelli inseriti in copia conoscenza.

La seconda tipologia è quella breve: come riportato nelle regole tecniche, "al fine di consentire uno snellimento dei flussi, è possibile, per il mittente, richiedere la ricevuta di avvenuta consegna in formato breve. La ricevuta di avvenuta consegna breve inserisce al suo interno il messaggio originale, sostituendone gli allegati con i relativi hash crittografici per ridurre le dimensioni della ricevuta. Per permettere la verifica dei contenuti trasmessi è indispensabile che il mittente conservi gli originali immodificati degli allegati inseriti nel messaggio originale, a cui gli hash fanno riferimento".

La terza tipologia è quella sintetica: in questo caso, nella ricevuta non c'è traccia del messaggio, ma vi è esclusivamente il file XML contenente i dati di certificazione. Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera un avviso di mancata consegna da restituire al mittente con l'indicazione dell'errore riscontrato.

Tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna sono caratterizzate dalla presenza di un riferimento temporale, che consente di provare a terzi l'esistenza di un determinato evento informatico in un certo momento.

Un altro aspetto rilevante, che riguarda l'intero sistema di posta elettronica certificata, è relativo all'architettura tecnico/funzionale che deve impedire che la presenza di virus possa compromettere la sicurezza di tutti i possibili messaggi gestiti; deve quindi essere prevista l'istallazione ed il costante aggiornamento di sistemi antivirus che impediscano quanto più possibile ogni infezione, senza però intervenire sul contenuto della posta certificata.

In particolare, ai sensi dell'articolo 11 del D.M. 2 novembre 2005, il gestore è tenuto ad informare il mittente che il messaggio inviato contiene virus, messaggio che dovrà essere conservato per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle deliberazioni del CNIPA (oggi, Digit-

PA) in materia di riproduzione e conservazione dei documenti su supporto ottico.

Infine, va ricordato che il gestore PEC è tenuto ad informare il cliente se la posta in arrivo non è qualificabile come posta elettronica certificata e, nel caso in cui l'utenza sia stata impostata in modo da poter ricevere anche messaggi non-PEC, deve inserire la stessa in una busta c.d. di anomalia grazie alla quale sarà possibile distinguere immediatamente il carattere "ordinario" del messaggio ricevuto.

Il D.P.R. 68/2008 nel disciplinare gli effetti legali della trasmissione di un messaggio mediante posta elettronica certificata aveva operato una scelta volta ad escludere ogni automatismo nella loro produzione.

Per i privati cittadini, infatti, il solo indirizzo valido, ad ogni effetto giuridico, sarebbe stato quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi e le pubbliche amministrazioni.

La predetta dichiarazione di volontà, peraltro, non avrebbe potuto comunque dedursi dalla mera indicazione dell'indirizzo di posta elettronica certificata nella corrispondenza o in altre comunicazioni o pubblicazioni del soggetto (ad esempio, nel proprio blog personale, o nel profilo di un social network ecc.).

Un'eccezione era rappresentata dalla possibilità per le imprese di esplicitare la volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione nel registro delle imprese.

Appare di tutta evidenza come l'impianto normativo fosse ispirato da una forte prudenza, tale però da apparire eccessiva e rendere particolarmente farraginoso l'utilizzo di uno strumento nuovo e che, dunque, già di per sé avrebbe dovuto scontare la naturale diffidenza degli utenti.[Fab]

Sul punto, pertanto, decisivo è stato l'intervento operato con gli articoli 16 e 16-bis del D.L. 185/2008, convertito in legge 2/2009, i quali hanno contribuito, non senza sollevare polemiche, a rendere più facile l'utilizzo della posta elettronica certificata, rendendo automatica per talune categorie la

produzione degli effetti giuridici ad essa collegati[15].

In particolare l'articolo 16 ha disposto, in primo luogo, l'obbligo per le imprese costituite in forma societaria, nonché per i professionisti iscritti in albi o elenchi istituiti con legge dello Stato (ad esempio, avvocati, medici, ingegneri) di dotarsi di un indirizzo di posta elettronica certificata da comunicare rispettivamente al registro delle imprese e al proprio ordine professionale di appartenenza.

In conseguenza dell'obbligo predetto le comunicazioni tra i soggetti di cui sopra e tra gli stessi e la Pubblica Amministrazione possono essere inviate attraverso la posta elettronica certificata, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo: dunque, una netta inversione di tendenza rispetto alla scelta operata nel 2005.

L'articolo 16-bis della medesima legge ha dato ingresso nel nostro ordinamento a quella che può essere definita come PEC di Stato[16].[Lon] Si è previsto, infatti, che "per favorire la realizzazione degli obiettivi di massima diffusione delle tecnologie telematiche nelle comunicazioni ai cittadini che ne fanno richiesta è attribuita una casella di posta elettronica certificata il cui utilizzo abbia effetto equivalente, ove necessario, alla notificazione per mezzo della posta".

Nella stessa disposizione si rimandava ad un Decreto della Presidenza del Consiglio dei Ministri per la definizione delle modalità di rilascio e di uso della casella di Postale Elettronica, che veniva adottato il 6 maggio 2009.

Nel Decreto si specifica che al cittadino che ne fa richiesta la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie-, direttamente o tramite l'affidatario del servizio, assegna un indirizzo di PEC, il quale diverrà l'indirizzo valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni. La richiesta di attivazione del predetto indirizzo comporta per il cittadino la esplicita accettazione dell'invio, tramite

[15]Sulla stessa scia, si è inserito di recente il D.lgs n. 235 del 30 dicembre 2010 che ha recato profonde modifiche al d.lgs 82/2005.

[16] T. De Longo: "La Pec gratuita ai cittadini non è un'invenzione di Brunetta"

PEC, da parte delle pubbliche amministrazioni di tutti i provvedimenti e gli atti che lo riguardano.

La strada intrapresa con la legge 2/2009, tendente al superamento del principio del consenso preventivo di cui all'articolo 4, commi 2 e 3, D.P.R. 68/2005, ha trovato il suo punto di arrivo nel recentissimo D.lgs 235/2010 che, all'articolo 56, ha abrogato i commi sopra citati, consegnando, tuttavia, all'operatore del diritto uno scenario ancora una volta non privo di incertezze.

In primo luogo, è agevole notare come l'abrogazione non abbia riguardato il comma 5 del medesimo articolo nel quale si specifica che "le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione della disponibilità, nonché le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17".

La ragione è da rinvenirsi, a parere di chi scrive, nella nuova formulazione dell'articolo 6, comma 1, del Codice dell'Amministrazione Digitale (come modificato dall'articolo 5, comma 1, D.lgs 235/2010) che, limitatamente ai rapporti cittadino-Pubblica Amministrazione, stabilisce che "1. Per le comunicazioni di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni degli atti e dei provvedimenti che lo riguardano".

Dunque, per quel che concerne i rapporti con la PA, l'utilizzo della PEC necessiterà sempre del preventivo consenso dell'interessato, che potrà intervenire in sede di sottoscrizione del contratto di attivazione della c.d PEC di stato (rectius, CEC-PAC), oppure potrà essere prestato secondo le modalità indicate nella normativa tecnica.

Con riferimento a tale ultima ipotesi va sottolineata la circostanza che

l'unico riferimento rinvenibile nella regolamentazione tecnica in merito alla comunicazione ed alla variazione della disponibilità di utilizzo della posta elettronica certificata appare essere quello di cui all'articolo 5, D.M. 2 novembre 2005, il quale recita:

"1.La dichiarazione di cui all'articolo 4, comma 4, del D.P.R. n. 68 del 2005, può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del D.P.R. n. 445 del 2000. 2. La dichiarazione di cui al comma 1 è resa anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima".

Orbene, come noto, il comma 4 citato è stato abrogato dal D.L. 185/2008, convertito in legge n. 2/2009: per l'effetto, sembra mancare del tutto nel nostro ordinamento una norma tecnica in grado di regolamentare quanto previsto dal richiamato art. 6, comma 1, CAD.

Altra conseguenza dell'abrogazione sopra menzionata è che un'esplicita dichiarazione di disponibilità a ricevere comunicazioni a mezzo PEC non risulta più necessaria nel caso dei rapporti giuridici tra privati cittadini: viene esteso, pertanto, l'automatismo già previsto dalla legge 2/2009 con riferimento alle sole comunicazioni tra società e professionisti e tra questi e le pubbliche amministrazioni.

A questo punto è lecito ipotizzare che qualsivoglia indicazione di un proprio indirizzo di posta elettronica certificata (sul proprio sito internet, su un profilo facebook o di altro social network, o anche sul proprio biglietto da visita) determini un'elezione di "domicilio informatico" nei rapporti tra privati.

Occorre ricordare che in sede di conversione in legge del D.L. 185/2008, è stata inserita, all'interno dell'articolo 16, una alternativa alla Posta Elettronica Certificata, giacché si è stabilito che le imprese e i professionisti, in luogo dell'indirizzo PEC, possono comunicare ai soggetti preposti "analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora

dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali".

Quest'ultima disposizione è connessa al fatto che la PEC è un sistema funzionante solo all'interno del territorio Italiano. Come si può notare, la norma non individua uno specifico sistema alternativo di posta alla PEC, ma indica i requisiti che esso deve soddisfare. In particolare, il sistema di posta elettronica deve essere basato su tecnologie che certificano la data e l'ora dell'invio e della ricezione delle comunicazioni e l'integrità del loro contenuto; esso inoltre deve assicurare l'interoperabilità con analoghi sistemi internazionali. Si segnala che la legge 18 giugno 2009, n 69, "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile" ha previsto che il Governo adotti un regolamento di modifica del regolamento sulla posta elettronica certificata, anche al fine di garantire l'interoperabilità di quest'ultima con analoghi sistemi internazionali.

Tuttavia, la possibilità di utilizzare sistemi alternativi alla PEC ha di recente trovato ingresso finanche nel Codice dell'Amministrazione Digitale, grazie alle modifiche introdotte all'articolo 48 dal D.lgs 235/2005, il cui primo comma ora è stato così riformulato: "la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA".

Ancora una volta, dunque, si dovrà attendere l'adozione di apposito decreto che garantisca l'operatività della norma citata la quale, al momento, appare sprovvista di portata immediatamente precettiva.

Quindi, grazie a quanto esposto finora, si può dedurre che l'uso della posta elettronica certificata possa oggi beneficiare di un quadro normativo complesso ma solido quanto meno nei rapporti tra privati e tra questi e le pubbliche amministrazioni.

Lo stesso dicasi per quanto concerne l'attività forense limitatamente agli

aspetti stragiudiziali.

Più tortuoso si rivela invece il cammino da percorre per l'uso della PEC in ambito processuale[17] e ciò per una duplice ragione: da un lato si assiste all'inerzia del legislatore rispetto all'adozione della normativa tecnica indispensabile per garantire l'operatività di norme esistenti ma consegnate ad una sorta di limbo.

Dall'altro ci sono ritrosia culturale, pigrizia mentale, scetticismo "tecnofobo" che portano (soprattutto tra gli avvocati) ad evidenziare unicamente i lati negativi della PEC, le eventuali problematiche legate alla sicurezza e alla gestione del documento informatico, piuttosto che a guardare ai vantaggi in termini di tempo e di libertà di azione che conseguirebbero dal suo uso quotidiano.

C'è da sperare, allora, che coloro i quali oggi si presentano come profeti di sventura possano in futuro essere ricordati per avere avuto lo stesso grado di lungimiranza che nel 1882 mostrarono alcuni impiegati della Western Union che in una comunicazione interna così si esprimevamo: "Questo cosiddetto "telefono" ha troppi difetti per poterlo considerare seriamente come mezzo di comunicazione. Il dispositivo è intrinsecamente privo di valore, per quel che ci riguarda".

Per fortuna altri la pensarono diversamente.

[17] Sul punto si segnala la recente presa di posizione della Corte Costituzionale che, con sentenza 22 dicembre 2010, n. 365,

Capitolo 4

PEC E Privacy

Dopo l'analisi dei principali mezzi attraverso i quali viene realizzata la comunicazione in ambito di pubbliche amministrazioni, spostiamo ora l'attenzione su alcuni aspetti giuridici in cui sono coinvolti. Al di là di definirli in questo ambito, passiamo ora a considerare alcune "complicazioni" derivanti dall'uso di questi: parleremo di trattamento di dati personali, accenneremo brevemente di reati informatici attuabili a mezzo di tali strumenti e infine affronteremo l'argomento sicurezza.

La globalizzazione dei mercati e la rapida diffusione delle nuove tecnologie, legate al mondo dell'informatica e delle telecomunicazioni, hanno inciso in modo sostanziale sul funzionamento dei sistemi economici di tutti paesi e sulla vita del singolo cittadino.

I cambiamenti si sono manifestati in vario modo: modificando i paradigmi produttivi, intensificando la velocità dei processi d'innovazione, trasformando i consumi, mutando i canali di comunicazione e del trasferimento delle informazioni.

I sistemi informativi, dopo la "rivoluzione telematica", diventano il necessario substrato, il tessuto connettivo essenziale e principale della nuova società che acquista, produce, vende e distribuisce nella realtà parallela, dove si traspone la propria personalità, delineando la nuova "società

dell'informazione"[1].[Leo]

Si scorgono,così, i tratti di una nuova cittadinanza, costruita proprio nella nuova dimensione definita dalle tecnologie dell'informazione e della comunicazione, dove l'insieme dei diritti dei cittadini sono, sempre più, condizionati dalla loro possibilità d'essere attori nei processi di comunicazione, e, non, soltanto, passivi fornitori di dati.

Nel 1999 due settimanali mondiali, "The Economist" e "Der Spiegel", dettero alle loro copertine un titolo significativo "Fine della Privacy", indagando minuziosamente sulle infinite tecniche di raccolta delle informazioni personali messe a punto dal sistema mondiale delle imprese, spesso, all' insaputa degli interessati.

E' necessario, pertanto, misurarsi con le tecniche della "New economy" che, bisognosa di dettagliatissime informazioni sulle persone e sui loro comportamenti, ne sollecita la cessione agli stessi interessati nella quotidianeità, facendone l'inevitabile contropartita di un servizio o di un beneficio. Tali informazioni diventano non solo gli strumenti che orientano le attività delle imprese, ma anche l'oggetto di un commercio sempre più fiorente. E' utile, inoltre, far rilevare che coloro i quali vengono a contatto con i dati concernenti la privacy hanno la possibilità d'interferenza nella vita privata degli interessati e di tenere,anche, comportamenti, potenzialmente, discriminatori.

E', pertanto, essenziale rafforzare il diritto all'autodeterminazione informativa da parte dei cittadini, consapevoli dell'illegittimità di ogni trattamento "invisibile" in rete e del pericolo di sottrarre al controllo degli interessati il complesso dei trattamenti che riguardano i propri dati personali[2] da parte dei violatori della privacy. [Fil02]

[1] "Internet e le nuove frontiere di tutela della privacy" articolo del dottoressa Francesca Leotta pubblicato su diritto.it

[2] "La centralità dell'informazione e della conoscenza per il funzionamento dei sistemi economici: il problema della società della classificazione" di Claudio Filippi e "Il diritto della nuova economia: e-business, copyright, diritti dei consumatori", a cura di Francesco Maschio, Padova 2002.

4.1 L'indirizzo e-mail come dato personale

"Internet si fonda sulla cooperazione tra sistemi privati. L'invio della posta elettronica è un privilegio, non un diritto" - John F. Hall-in news.admin.net-abuse e-mail - Tra i diritti della personalità tutelati dalla Costituzione, vi è la libertà e la segretezza dell'espressione del pensiero; in particolare l'art. 15 sancisce l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione.

Dal combinato esposto di questo articolo e degli altri articoli che garantiscono le singole manifestazioni in cui si esplica il diritto alla riservatezza se ne ricava, per derivazione, la sua tutela costituzionale.

Partiamo innanzitutto col fornire un po di definizioni:

- "trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;

- "dato personale": qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- "dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato;

- "dati sensibili": 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 od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

In passato il concetto di diritto alla riservatezza e di diritto della privacy venivano spesso usati in maniera analoga; con il d.lgs. 196/2003 il legislatore ne ha codificato la differenza definendo il diritto alla riservatezza come il diritto di ciascuno alla tutela di quelle situazioni personali o familiari svoltesi anche al di fuori del domicilio domestico che non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze non giustificate da interessi pubblici prevalenti, anche se lecite e tali da non offendere il decoro e l'onore. Questo diritto non può essere negato ad alcuna categoria di persone, solo in considerazione della loro notorietà, salvo che un reale interesse sociale all'informazione o altre esigenze pubbliche lo esigano.

Il diritto alla privacy invece consiste nel diritto di ciascuno di controllare la circolazione delle informazione riguardanti la propria persona[3].[Imp04]

All'art. 4 del suddetto testo normativo sono raccolti e definiti i termini utilizzati dal legislatore tra cui anche quello di dato personale inteso come "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

In materia di posta elettronica si può certamente asserire che l'indirizzo elettronico è un dato personale poiché risponde pienamente ai requisiti indicati dall'articolo suddetto.

L'indirizzo e-mail infatti è un informazione che può riferirsi sia a persona fisica che a persona giuridica e che, tramite il raffronto con alti dati, è idoneo (direttamente o indirettamente) all'individuazione del soggetto al quale le informazioni si riferiscono[4].

Per questi motivi, anche nell'ambito della posta elettronica possono essere richiamate, oltre a quelle proprie che riguardano le comunicazioni elettroniche, anche tutte quelle norme che si occupano di tutelare i dati personali e il loro trattamento.

[3]Si legga in proposito C. Cevenini, C. Di Cocco, G. Sartor, lezioni di informatica giuridica, 2005 Gedit Bologna

[4]Si veda al riguardo , R. Imperiali, codice della privacy: commento alla normativa sulla protezione dei dati personali, 2004, il sole 24 ore, Milano

Molto significativo a riguardo è un articolo riportato da M. Cammarata, su www.interlex.it, in cui si fa riferimento proprio all'indirizzo e-mail come dato personale[Cam03]: "Gli indirizzi di posta elettronica non sono liberamente utilizzabili da chiunque per il solo fatto di trovarsi in rete. La vasta conoscibilità degli indirizzi e-mail che Internet consente, non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line. Gli indirizzi e-mail non sono, insomma, "pubblici" come possono essere quelli presenti sugli elenchi telefonici.

Il principio è stato ribadito dall'Autorità Garante (composta da Stefano Rodotà. Giuseppe Santaniello, Gaetano Rasi e Mauro Paissan) che ha affrontato in questi ultimi mesi diversi casi di utenti che avevano segnalato la pratica ormai diffusa di inviare e-mail commerciali ad indirizzi di posta elettronica raccolti in rete. Alle proteste degli utenti, le società che avevano inviato le e-mail rispondevano che non vi era stata alcuna violazione della privacy perché gli indirizzi erano stati reperiti su Internet (spesso attraverso appositi software) e che pertanto erano "pubblici".

Niente di più sbagliato, afferma l'Autorità. Gli indirizzi di posta elettronica non provengono, infatti, da pubblici registri, elenchi, atti o documenti formati o tenuti da uno o più soggetti pubblici e non sono sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque. La circostanza che l'indirizzo e-mail sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti non lo rende, infatti, liberamente utilizzabile e non autorizza comunque l'invio di informazioni, di qualunque genere, anche se non specificamente a carattere commerciale o promozionale, senza un preventivo consenso.

L'Autorità sottolinea che l'eventuale disponibilità in Internet di indirizzi di posta elettronica, anche se resi conoscibili dagli interessati per certi scopi (ad esempio su un sito istituzionale o anche aziendale) attraverso siti web o newsgroup, va "rapportata alle finalità per cui essi sono pubblicati sulla rete".

A maggior ragione questo principio vale in caso di uso indebito di software

che rastrellano automaticamente migliaia di indirizzi in rete o li creano a tavolino a prescindere da un accertamento sulla loro effettiva esistenza.

Per poter inviare e-mail senza violare la privacy degli utenti web è obbligatorio, dunque, ottenere prima il loro consenso.

Uno degli ultimi casi di cui si è occupato il collegio del Garante ha riguardato un docente che si era visto recapitare una e-mail pubblicitaria al proprio indirizzo di posta elettronica, presente per finalità di istituto, sul sito dell'università presso la quale insegna."

A rafforzare quanto finora detto, dunque, ancora di più questo articolo ribadisce che un indirizzo di posta elettronica costituisce pienamente un dato personale relativo a persona e, in quanto tale, risponde alla giurisdizione in merito.

Il Garante per la Privacy, in un'ordinanza-ingiunzione del 18 settembre 2008, ha precisato che l'indirizzo di posta elettronica, benché non espressamente indicati nella definizione di "dato personale", contenuta nell'art. 4, comma 1, lett. b) del d. lgs. 196/2003 (Codice per la privacy), rappresentano certamente informazioni relative "a persona fisica, persona giuridica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione". A questo proposito, prosegue il Garante, è sufficiente considerare che una specifica sezione del Codice (Titolo X) è dedicata proprio alla disciplina dei trattamenti dei dati personali mediante le comunicazioni elettroniche.

Riporto l'ingiunzione da parte del Garante (da www.garanteprivacy.it)[urlg]:

"...Ritenuto che le argomentazioni addotte dalla società non risultano idonee in relazione alla contestazione della violazione amministrativa per omessa o inidonea informativa agli interessati in quanto:

1. indicare, da parte della società, che "l'utilizzo del numero di cellulare verrà utilizzato esclusivamente per un contatto telefonico di un nostro commerciale" non consente all'interessato di conoscere compiutamente e preventivamente le modalità del trattamento (art. 13, comma 1, lett. a)), la natura obbligatoria o facoltativa del conferimento dati (art. 13,

comma 1, lett. b)), le conseguenze di un eventuale rifiuto di rispondere (art. 13, comma 1, lett. c)), i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venire a conoscenza in qualità di responsabili o di incaricati (art. 13, comma 1, lett. d)) (al riguardo, anche l'indicazione di "un nostro commerciale" deve ritenersi inidonea attesa la sua assoluta genericità), i diritti di cui all'art. 7 (art. 13, comma 1, lett. e)), nonché gli estremi identificativi del titolare (art. 13, comma 1, lett. f)) (al riguardo, la mera indicazione "Soc. Universitalia" non consente, nel caso di specie, un'individuazione certa del titolare del trattamento, non essendo indicata la ragione sociale completa accompagnata da un idoneo recapito. In ogni caso, nessuna delle predette informazioni viene fornita con riferimento al trattamento dell'indirizzo di posta elettronica;

2. la nozione di dato personale, che la società ritiene di poter evincere dall'art. 4, comma 1, lett. b) del Codice, è erronea, atteso che il numero di telefonia mobile e l'indirizzo di posta elettronica rappresentano certamente informazioni relative a persona fisica, persona giuridica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione; a riprova di ciò, va rilevato che una specifica sezione del Codice (Titolo X) è dedicata proprio alla disciplina dei trattamenti dei dati personali mediante le comunicazioni elettroniche. Risulta, pertanto, irrilevante che il predetto art. 4, comma 1, lett. b) non elenchi esplicitamente le tipologie di dati personali;"

La società in merito venne condannata a pagare un somma di seimila euro di sanzione per la violazione dell'articolo 161, e quindi ancora di più si rafforzava l'idea di dato personale in merito alla posta elettronica.

In conclusione di questo paragrafo, dobbiamo dire che la posta elettronica rientra nelle corrispondenze protette dall'articolo 15 della Costituzione e nella tutela approntata (art. 615, 618 e seguenti del codice penale) in favore della corrispondenza epistolare o telefonica.

In quest'ottica, le norme che tutelano la riservatezza della corrispondenza si applicano anche in ambito aziendale, e a prescindere da chi sia il proprietario dei mezzi utilizzati per effettuare corrispondenze e comunicazioni, si ha il diritto a mantenerle segrete.

4.2 Il trattamento dei dati personali

A livello europeo un intervento significativo in materia di trattamento dei dati personali è stato eseguito con la direttiva 2002/58 CE del 12 luglio 2002 che si pone come obbiettivo la tutela della vita privata nello specifico settore delle comunicazioni elettroniche.

La direttiva aveva come scopa l'armonizzazione delle disposizioni degli Stati membri nella misura necessaria per assicurare un livello omogeneo di tutela dei diritti e delle libertà fondamentali, in particolare per quel che riguardava il trattamento dei dati personali nel settore delle comunicazioni elettroniche e la loro libera circolazione all'interno della Comunità[5].

Il considerando n.6 del provvedimento in questione[6] evidenziò in modo particolare come i servizi di comunicazione elettronica, accessibili grazie all'uso di internet, furono per gli utenti, da un lato, dei mezzi facilmente utilizzabili, ma dall'altro, rappresentarono nuovi pericoli per i loro dati personali e per la loro vita privata.

[5]Si riporta il testo dell'art. 1, comma 1 della direttiva 2002/58 CE:"la presente direttiva armonizza le disposizioni degli Stati membri necessarie ad assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità"

[6]Si riporta quanto detto nel considerando n.6 della direttiva 2002/58 CE: "l'internet ha sconvolto le tradizionali strutture del mercato fornendo un infrastruttura mondiale comune per la fornitura di un ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e pera la loro vita privata"

Con l'art. 4 la direttiva pose l'accento sugli aspetti che riguardavano la sicurezza dei servizi di comunicazione ed il considerando n. 20 specificò che "è di particolare importanza per gli utenti e gli abbonati di tali servizi essere informati pienamente dal loro fornitore di servizi dell'esistenza di rischi alla sicurezza al di fuori della portata dei possibili rimedi esperibili dal fornitore stesso. I fornitori di servizio che offrono servizi di comunicazione elettronica accessibili al pubblico su internet dovrebbero informare gli utenti e gli abbonati delle misure che questi ultimi possono prendere per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecniche di criptazione. L'obbligo di informare gli abbonati sui particolari rischi relativi alla sicurezza non esonera il fornitore di servizi dall'obbligo di prendere, a sue proprie spese, provvedimenti immediati ed adeguati per rimediare a tutti i nuovi imprevisti o rischi relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio."

L'art. 5 invece si occupò degli aspetti riguardanti la riservatezza delle comunicazioni per ottemperare l'esigenza di "prendere misure per prevenire l'accesso non autorizzato alle comunicazioni al fine di tutelare la riservatezza delle comunicazioni realizzate attraverso reti pubbliche di comunicazione e servizi di comunicazione elettronica accessibili al pubblico compreso il loro contenuto e qualsiasi dato ad esse relativo" secondo il considerando 21.

A livello nazionale l'argomento in esame si rifece al d.lgsl. n. 196/2003, Testo Unico delle norme legislative in materia di protezione dei dati personali[7].

L'articolo 11 del suddetto testo normativo raccolse i principi generali a cui ogni trattamento di dati personali doveva conformarsi e cioè i principi di liceità e correttezza, i quali richiedevano, e tuttora richiedono, per un corretto adeguamento, una valutazione che doveva andare oltre l'analisi delle sole norme in materia di protezione dei dati personali rifacendosi alle disposizioni di tutto l'ordinamento giuridico e al più generale rispetto delle regole, anche

[7]Il T.U. In materia di privacy raccolse al suo interno la precedente legge n. 675/1996 che attuò la direttiva 1995/46 CE

di quelle non codificate.

In modo particolare le operazioni di raccolta e registrazione dei dati dovevano avvenire per scopi determinati, espliciti e legittimi; l'interessato doveva quindi essere a conoscenza delle specifiche finalità per le quali si procedeva al trattamento.

Gli stessi dati, d'altra parte, dovevano soddisfare il requisito dell'esattezza ed essere "pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati"; all'esattezza dei dati si ricollegava il dovere di aggiornamento degli stessi, dal momento che dati non aggiornati corrispondevano nella sostanza a dati non esatti[8].

Una volta raggiunto lo scopo per il quale i dati sono stati raccolti e successivamente trattati, essi dovevano essere resi anonimi o, comunque, cancellati; l'interessato aveva, cioè, l'obbligo ad essere dimenticato[9].[GC04]

Prima ancora di procedere alla raccolta dei dati personali, il titolare era tenuto ad informare l'interessato della tipologia di trattamento a cui i propri dati erano destinati, in modo tale da consentire a quest'ultimo la possibilità di espressione di consenso.

L'informativa era disciplinata all'articolo 13 del d.lgsl. 196/2003 poteva essere fornita per iscritto oppure oralmente, ma doveva necessariamente contenere tutte le informazioni relative all'identificazione del trattamento.

L'interessato o la persona presso i quali vengono raccolti i dati personali dovevano essere posti a conoscenza delle finalità e delle modalità del trattamento cui erano destinati i dati e, soprattutto, dovevano essere avvisati della natura obbligatoria o facoltativa del conferimento dei dati.

Essi, inoltre, dovevano avere la possibilità di sapere quali fossero le conseguenze nel caso rifiutassero di rispondere; di conoscere i soggetti ai quali i

[8]Si veda in proposito G. Cassano, S. Fadda, codice in materia di protezione dei dati personali: commento articolo per articolo al Testo Unico sulla privacy D.lgsl. 30 giugno 2003, 2004 IPSOA, Milano

[9]Si veda in proposito G. Cassano, S. Fadda, codice in materia di protezione dei dati personali: commento articolo per articolo al Testo Unico sulla privacy D.lgsl. 30 giugno 2003, 2004 IPSOA, Milano

dati personali potevano essere comunicati o che, comunque, potevano venirne a conoscenza in qualità di responsabili o incaricati e di essere informati circa l'ambito di diffusione dei dati medesimi.

L'informativa doveva poi contenere il riferimento alla possibilità per l'interessato di esercitare il diritto di accesso e gli altri diritti previsti dall'art. 7, nonché i dati identificativi del titolare e di almeno un responsabile.

L'articolo 23 del Testo Unico disponeva che "il trattamento dei dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato", salvi i casi di esclusione del consenso di cui all'articolo 24 della legge.

Ai sensi della medesima disposizione, il consenso era validamente prestato solo se espresso liberamente, in forma specifica e documentata per iscritto, e se erano rese all'interessato le informazioni di cui all'articolo 13 della legge.

Il consenso doveva essere prestato prima dell'inizio del trattamento e dopo aver avuto conoscenza dell'informativa a pena di nullità.

In materia di sicurezza di dati il Testo Unico prevedeva all'articolo 31 l'obbligo di adottare, mediante misure idonee e preventive, tutti quegli accorgimenti suggeriti dalle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

La sicurezza riguardava i dati trattati, e la protezione del sistema informatico era il mezzo attraverso il quale si esplicava.

Gli articoli 33 e successivi individuavano invece in modo tassativo le misure minime di sicurezza che furono definite in relazione alla natura media dei trattamenti.

La mancata adozione delle misure di cui all'articolo 31, determinava responsabilità civile con relativo risarcimento, mentre la mancata adozione delle misure minime veniva sanzionata penalmente.

L'articolo 32 si occupò di disciplinare le misure tecniche e organizzative che dovevano essere adottate da particolari titolari di fornitura di servizi, in modo particolare per quel che riguardava l'uso di internet e ai fenomeni ad esso connessi.

Quindi si può notare come già in passato la legislazione abbia cercato di dare un impronta forte sul trattamento dei dati personali, per cui si invitava già le persone ad una cauta ed attenta lettura di informative che troppo spesso, venivano e tuttora, vengono ignorate da un semplice "click" sul pulsante "Accetto".

Passiamo ora il focus sulla normativa vigente in merito all'argomento.

Sostanzialmente le normative vigenti sono quelle finora affrontate, ma porterò all'attenzione alcune modifiche necessarie per comprendere l'evoluzione normativa.

Interessante è a proposito un articolo pubblicato su interlex (www.interlex.it) da parte di C. Giustozzi in merito ad alcune modifiche apportate sulla questione privacy dal garante[Giu09]: "No, non sto pensando al vento ed al maltempo che pure, durante le ultime settimane del concluso 2008, hanno infierito sul nostro Paese. Mi riferisco invece alla gragnuola di importanti provvedimenti che il Garante ha prodotto in fine d'anno e che oltretutto, per effetto forse del caso o magari delle oscure forze del male che sembrano spesso sovraintendere le questioni legate alla privacy, sono passate inosservate ai più, in quanto finite in Gazzetta Ufficiale a ridosso o addirittura proprio nel bel mezzo delle festività invernali. Mi riferisco in particolare al provvedimento del 13 ottobre 2008 (pubblicato in G.U. n. 287 del 9 dicembre 2008) relativo a "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali", al provvedimento del 27 novembre 2008 (pubblicato nella medesima G.U. n. 287 del 9 dicembre 2008) relativo a "Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali" ed al provvedimento sempre del 27 novembre 2008 (pubblicato però in G.U. n. 300 del 24 dicembre 2008) relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Si tratta di tre provvedimenti importanti non solo per le evidenti implicazioni di natura giuridica, e quindi già ampiamente commentate in quanto

tali su queste colonne, ma anche se non soprattutto per le questioni di natura tecnica che affrontano. Tutti i lettori di InterLex sanno molto bene quanto spesso e con quale profondità di rapporti l'esercizio e la tutela della privacy si intersechino con le tecnologie dell'informazione, viste talvolta come alleate e talaltra come avversarie; e quanto il Garante sia sensibile (a volte perfino troppo...) ai rischi cui le tecnologie informatiche, laddove vengano usate con scarsa attenzione e consapevolezza, possono potenzialmente esporre i dati personali oggetto di tutela da parte della legge.

È dunque piuttosto importante analizzare proprio sul piano tecnico-informatico questi recenti provvedimenti, i quali introducono non banali innovazioni nel corpus normativo che regola la gestione informatica dei dati personali, per capire in ultima analisi cosa occorre fare (o non fare) in pratica per mettersi (o rimanere) in regola con quanto richiesto dalla legge. La quale, va detto, appare sempre più attenta e stringente anche su questioni che fino a qualche anno fa sarebbero apparse del tutto estranee alla maggior parte degli operatori del diritto.....Forse per compensare un po' la meritoria operazione culturale compiuta con il precedente provvedimento, il Garante ha contestualmente provveduto ad emanare un provvedimento semplificativo che riduce notevolmente l'efficacia delle "misure minime" di sicurezza per talune categorie di soggetti titolari di trattamenti. Lo scopo era quello di alleviare la pressione tecnologica sui titolari "meno attrezzati" (artigiani, piccole aziende), ma la mia impressione è che in questo caso si sia voluto semplificare un po' troppo.

Al di là della difficoltà di stabilire chi di fatto possa godere di tale regime semplificativo, le nuove misure minime prevedono ora che il titolare possa impartire le istruzioni agli incaricati anche oralmente, che come sistema di autenticazione vada bene qualsiasi meccanismo basato su userid e password, che l'antivirus vada aggiornato una volta l'anno e il backup fatto una volta al mese. Anche il DPS può essere sostanzialmente semplificato.

Ora, sicuramente, l'intendimento del Garante era buono: considerando che la maggior causa delle inadempienze nell'applicazione delle misure minime da parte dei "piccoli operatori" veniva individuata proprio nella presunta

impossibilità di adottare rigorose misure tecniche, la loro attenuazione è stata evidentemente vista come incentivo alla messa in regola da parte di queste categorie. Tuttavia non si fa un buon servizio alle esigenze di crescita culturale della popolazione affermando che è sufficiente aggiornare un antivirus (o applicare le patch di sicurezza al sistema operativo) una volta all'anno; e addirittura ogni due anni se il computer non è connesso a reti di comunicazione pubbliche. Passi per il backup ogni mese, ma l'antivirus va aggiornato tassativamente tutte le volte che il produttore emette gli aggiornamenti, il che oramai significa anche due o tre volte al giorno...

E poi mi domando: se il titolare può impartire disposizioni in merito alla sicurezza anche solo oralmente, come farà in caso di eventuali contestazioni a dimostrare di averlo fatto? Ma costa davvero troppo in termini di sforzo intellettuale scrivere un documentino di una pagina con le procedure da seguire? E siamo sicuri che è solo per l'incapacità di sostenere questo sforzo che la maggior parte delle piccole aziende e degli studi professionali non è ancora in regola con la privacy?.

E veniamo infine brevemente all'ultimo provvedimento, quello che... resuscita la mitica figura dell'amministratore di sistema già presente nella prima legge sulla privacy e palesemente assente, sino ad oggi, da quella vigente.

L'amministratore è, come tutti sappiamo, il signore e padrone dei computer aziendali: a lui è infatti concesso svolgere quelle operazioni di gestione, controllo e manutenzione sui sistemi che ai comuni mortali solitamente non sono permesse in quanto richiedono grande esperienza e specifiche conoscenze tecniche. Un amministratore, per poter svolgere le sue funzioni, è solitamente immune alle limitazioni imposte agli utenti: ad esempio può accedere ai dati di tutti gli utenti, installare o disinstallare programmi, copiare e cancellare archivi, e così via.

In passato l'amministratore veniva definito superuser, il che la dice lunga sui suoi... super poteri. In conseguenza di tali necessarie ma pericolose prerogative, la precedente legge sulla privacy giustamente riconosceva all'am-

ministratore di sistema un ruolo speciale di grande responsabilità, del quale egli non deve abusare (la stessa cosa ad esempio è prevista dal codice penale laddove si tratta di reati informatici). Tale ruolo, non presente nella formulazione originale del DLGV 196/03, viene ora in esso reintrodotto dall'ultimo dei tre provvedimenti di cui ci stiamo occupando.

Si tratta come si vede di un ripensamento tardivo, pensato per correggere una visibile stortura della legge ma che, per il modo in cui è formulato, finirà forse per complicare più del necessario la vita a coloro che dovranno attuarlo. Allo scopo di responsabilizzare al massimo gli amministratori di sistema, e sensibilizzare i titolari sulla necessità di controllarne le azioni, il Garante ha infatti dettato una serie di requisiti tecnici di difficile ed onerosa adozione, stabilendo oltretutto un termine di soli quattro mesi per la loro introduzione in esercizio. Non si tratta di un compito semplice, e temiamo che non saranno molte le aziende in grado di mettersi compiutamente in regola nei modi e nei tempi previsti.

Uno dei problemi maggiori è quello del controllo dell'attività dell'amministratore di sistema. Già per definizione tale attività è difficilmente controllabile, nel senso di "rilevabile e registrabile", proprio per via delle prerogative stesse della figura di amministratore: non tutte le azioni che un amministratore fa vengono infatti registrate dal sistema, anche perché molte di esse avvengono di necessità per vie non usuali (ad esempio l'accesso ad una base di dati senza passare dalle funzionalità applicative).

Ma il Garante non chiede solo di tracciare tutti gli accessi logici ai sistemi ed agli archivi, cosa che spesso non è tecnicamente possibile: per di più vuole anche che le relative registrazioni abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Ciò di fatto significa che i log dell'attività dell'amministratore, ammesso che siano generati dal sistema con la necessaria granularità, non possono essere memorizzati sul sistema stesso dove sta operando l'amministratore ma debbono essere immediatamente inviati ad un server esterno che li marchi

temporalmente, li firmi digitalmente e li archivi in modo inalterabile. Cosa che ovviamente si può fare, ma è certamente molto onerosa sia in termini di impegno realizzativo sia, soprattutto di costo, particolarmente in quelle realtà ove vi sono decine o centinaia di server sottoposti ad amministrazione. In realtà del genere è facile presumere che non si possa ragionevolmente mettere in piedi una simile infrastruttura in soli quattro mesi, e comunque che il farlo possa comportare spese non indifferenti da parte dell'azienda per prodotti ed infrastrutture.

In questo caso dunque il Garante è stato forse un po' troppo precipitoso, imponendo con urgenza misure tecniche ed organizzative di difficile attuazione. Sarebbe stato meglio fornire tempi più lunghi, e magari graduare il provvedimento con rispetto alla dimensione e complessità delle specifiche organizzazioni chiamate ad adottarlo. Ma, si sa, non tutto è perduto: siamo in Italia, ed una proroga non si nega a nessuno: tante cose possono cambiare da qui ad aprile, chissà che un giorno prima della scadenza il Garante stesso non decida di posporre i termini per l'adozione del provvedimento."

In questo articolo dunque si profilano due aspetti di non poca importanza: viene in pratica, nel primo dei due provvedimenti, data la possibilità ai titolari di trattamenti di dati personali di poter comunicare le istruzioni agli incaricati anche oralmente; ora, secondo il mio modesto punto di vista, questa è una strada sbagliata da percorrere, visto che ai contratti di licenza esplicati in maniera chiara e soprattutto in forma scritta, viene data poca attenzione, quindi si può solo immaginare lo scenario di fronte a cui ci si può ritrovare in ambito orale. Credo sia giusto, da parte del legislatore, rivedere certe posizioni, per poter offrire servizi sempre migliori a coloro i quali si apprestano ad utilizzare certi servizi.

Nel secondo provvedimento invece, ci si riferisce alla reperibilità delle azioni di un amministratore di sistema; ebbene in questo caso, a differenza del precedente, ci troviamo di fronte ad un provvedimento che, a mio parere, risulta legittimo, ma che in ogni modo deve rivedere la propria attuazione: mi spiego meglio.

Se da un lato è giusto dover tener traccia delle attività di un amministratore di sistema, poiché è noto che i privilegi che lo riguardano differiscono da quelli dei normali utenti, dall'altro sono sbagliati i modi con cui il provvedimento tenta di agire: bisognerebbe semplificarli per riuscire ad ottenere una gestione più rapida, ma che in ogni caso risulti efficace. Ulteriore lavoro per il legislatore.

Passiamo ora invece ad analizzare un caso dei giorni nostri, ovvero una modifica del cosiddetto Decreto Sviluppo n. 70/2011, "Prime disposizioni urgenti per l'economia", saltato agli onori della cronaca per la "privatizzazione" delle spiagge; ebbene, tale decreto non reca solo modifiche appunto in ambito economico, ma tratta anche di argomenti inerenti la privacy e il trattamento dei dati personali.

In merito riporto un articolo pubblicato dalla prof.ssa Giusella Finocchiaro, reperibile sul proprio blog (http://www.blogstudiolegalefinocchiaro.it):

"Il decreto legge recante "Prime disposizioni urgenti per l'economia", c.d. "decreto sviluppo", esaminato dal Consiglio dei ministri il 5 maggio scorso e ancora suscettibile di modificazioni, che molto ha fatto discutere per le disposizioni concernenti le concessioni sulle spiagge, contiene anche alcune rilevanti modifiche al Codice per la protezione dei dati personali.

Di seguito, una breve sintesi delle principali.

Dati di persone giuridiche, enti o associazioni

Nel nuovo art. 3-bis si prevederebbe (il condizionale è d'obbligo) che il trattamento dei dati personali di persone giuridiche, enti o associazioni nell'ambito di comunicazioni fra questi soggetti e per finalità amministrativo-contabili, non sia più soggetto all'applicazione del Codice. Non verrebbe, dunque, sottratto all'ambito di applicazione del Codice qualunque dato concernente persone giuridiche, pubbliche o private, ma solo i dati:

1) concernenti persone giuridiche, enti, pubblici o privati, associazioni

2) trattati per comunicazioni fra questi soggetti

3) per finalità amministrativo-contabili.

Quindi, per esempio, i dati relativi alla fatturazione comunicati fra im-

prese per finalità amministrative.

Si tenga presente che la direttiva europea 46/95/CE si applica solo ai dati relativi a persone fisiche, e che una scelta diversa era stata effettuata dal legislatore italiano nel 1996.

Curricula di chi cerca lavoro

I curricula spontaneamente inviati da chi cerca lavoro non richiederebbero l'informativa del titolare, se non al primo contatto successivo all'invio del curriculum, anche in forma orale. Non sarebbe più necessario, in questi casi, il consenso di chi ha inviato il cv, anche se questo contenesse dati sensibili.

Consenso nei rapporti fra imprese

Non sarebbe più necessario il consenso alla comunicazione di dati fra imprese (in ambiti specificati) per finalità amministrativo – contabili.

Misure di sicurezza

I titolari che trattano come unici dati sensibili o giudiziari quelli relativi ai propri dipendenti e collaboratori, nonché ai coniugi e ai parenti di questi ultimi, non sarebbero tenuti alla compilazione del documento programmatico per la sicurezza, ma potrebbero ricorrere ad un'autocertificazione.

Il d.p.s., se i dati trattati non sono sensibili, non è dovuto neanche oggi e quindi è pleonastica la menzione che ne fa il decreto in questo caso.

L'autocertificazione, si ricorda, comporta comunque rilevanti conseguenze sul piano della responsabilità, anche penale.

Il Garante potrebbe semplificare ulteriormente in materia di sicurezza.

Sono precisate le finalità amministrativo-contabili nel nuovo art. 34-comma 1 ter.

Comunicazioni commerciali indesiderate

Come già per le comunicazioni telefoniche, il consenso non sarebbe più necessario e si estenderebbe il sistema dell'opt-out, con relativo registro delle opposizioni, anche alle comunicazioni postali."

Dalla lettura dell'articolo derivano un paio di considerazioni; la prima: si sta cercando in qualche modo di semplificare il trattamento dei dati personali, o meglio, si sta cercando di rendere l'iter della comunicazione meno gravoso

da parte di chi è tenuto a dare informazioni in merito. Se da un lato la semplificazione giova per tutto quello che riguarda le "burocrazie", dall'altro si corre il già citato rischio di dare sempre meno importanza a questi aspetti che, a mio parere, invece risultano di fondamentale valore. La seconda considerazione riguarda il campo del trattamento dei dati personali in generale; la materia è di ampio raggio, e credo che molti passi debbano ancora essere compiuti per far si che una legislazione chiara e precisa sia messa in atto. Si dovrebbe lavorare su più aspetti, e uno di questi riguarda anche la coscienza dei propri diritti e doveri da parte delle persone, ma in questo caso il legislatore ha poco lavoro da svolgere, in questi casi bisognerebbe lavorare su coscienza e senso civico, il che esula dal compito di quest'ultimo. In generale è comunque auspicabile un miglioramento della normativa vigente.

4.3 Comunicazioni indesiderate

L'articolo 13 del T.U. riprendendo il testo della direttiva 2002/58 CE si occupò delle comunicazioni indesiderate in genere, comprendendo anche le attività promozionali e i messaggi pubblicitari effettuati tramite e-mail.

Riporto di seguito il testo della direttiva:

1. "L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso.

2. Fatto salvo il paragrafo 1, allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, a condizione che ai clienti sia offerta in modo

chiaro e distinto al momento della raccolta delle coordinate elettroniche e ad ogni messaggio la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora il cliente non abbia rifiutato inizialmente tale uso.

3. Gli Stati membri adottano le misure appropriate per garantire che, gratuitamente, le comunicazioni indesiderate a scopo di commercializzazione diretta, in casi diversi da quelli di cui ai paragrafi 1 e 2, non siano permesse se manca il consenso degli abbonati interessati oppure se gli abbonati esprimono il desiderio di non ricevere questo tipo di chiamate; la scelta tra queste due possibilità è effettuata dalla normativa nazionale.

4. In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni.

5. Le disposizioni di cui ai paragrafi 1 e 3 si applicano agli abbonati che siano persone fisiche. Gli Stati membri garantiscono inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente alle comunicazioni indesiderate."

Secondo il comma 1 dell'articolo "l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è permesso previo consenso dell'interessato" ed il comma 2 precisa che quanto detto in precedenza si applicava anche alle comunicazioni elettroniche, effettuate anche mediante posta elettronica per le finalità ivi indicate.

Il legislatore ha, quindi, preferito il sistema del "opt-in" secondo il quale l'interessato poteva decidere preventivamente e in maniera positiva se au-

torizzare il futuro trattamento dei dati personali propri; con il sistema del "opt-out", invece, l'interessato si opponeva al trattamento dei dati personali che era però già in corso; a tale proposito è necessario precisare che sulla base della formulazione legislativa il ricorso all'opt-out non poteva sostituire il requisito del consenso esplicito perché, di fatto, i dati personali dell'interessato erano già stati fatti oggetto di trattamento da parte del titolare.

Il comma 4 dell'articolo in esame introdusse la possibilità per gli enti commerciali di utilizzare gli indirizzi e-mail forniti dai propri clienti nel corso di precedenti transazioni commerciali, allo scopo di commercializzare prodotti analoghi senza che l'interessato dovesse riaffermare il proprio consenso.

In altre parole, se il titolare del trattamento utilizzava, a fini di vendita diretta di propri prodotti o servizi, l'indirizzo e-mail già fornito dall'interessato nel contesto della vendita di un prodotto o di un servizio, poteva non richiedere il consenso dell'interessato sempre che questi, adeguatamente informato, non ne rifiutava tale uso, inizialmente o in occasione di successive comunicazioni[10].

Il comma 5 vietava, in ogni caso, l'invio di comunicazioni per le finalità indicate nel primo comma, o comunque, a scopo promozionale, camuffando o celando l'identità del mittente o senza che fosse fornito un idoneo recapito presso il quale l'interessato potesse esercitare i propri diritti.

Con il seguente testo, quindi, si è cercato di dare una prima impronta giuridica al problema delle comunicazioni indesiderate, ma come prevedibile, la normativa col passare del tempo ha subito delle modifiche, in quanto l'argomento riguarda strumenti che hanno anche loro subito una evoluzione tecnologica.

E' di qualche anno fa un chiarimento in merito da parte del Garante per la privacy in merito all'argomento:il Garante ha ribadito che l'uso di sistemi automatizzati di chiamata, senza l'intervento di un operatore, per l'invio di materiale pubblicitario o di vendita diretta o per il compimento

[10]Si legga a proposito R. Imperiali, codice della privacy: commento alla normativa sulla protezione dei dati personali

di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

Ciò significa che non si possono inviare e-mail, telefax, messaggi del tipo mms o sms per pubblicizzare un prodotto o un servizio, senza prima aver ottenuto il consenso del destinatario, anche quando si tratta solo del primo invio.

In particolare, nelle sue decisioni, l'Autorità ha spiegato che, se l'invio è a fini di pubblicità e marketing, occorre ottenere sempre il consenso del destinatario prima di effettuare qualunque uso del suo indirizzo di posta elettronica.

Infatti, viene precisato che l'uso dell'indirizzo di posta elettronica è soggetto all'obbligo di informativa e all'obbligo di acquisizione preventiva del consenso.

Ribadendo un principio fondamentale per l'uso degli indirizzi e-mail, l'Autorità ha poi sottolineato che un indirizzo di posta elettronica, per il solo fatto di essere reperibile in rete, non autorizza comunque un suo uso indiscriminato: in questo caso il loro utilizzo deve essere conforme alle finalità per cui essi sono pubblicati sulla rete.

E comunque, la conoscibilità di fatto dell'e-mail o di qualsiasi altro dato personale non rende legittimo l'invio di informazioni, di qualunque genere, anche se non specificatamente a carattere commerciale o promozionale, senza un preventivo consenso.

Stop anche agli applicativi in grado di raccogliere dalla rete gli indirizzi di posta elettronica.

"Occorre dire un fermo no - sostiene il Garante - alla prassi di mandare una mail pubblicitaria senza consenso e poi scusarsi affermando che comunque quella era l'unica comunicazione inviata. Così come bisogna smetterla con la prassi di reperire un indirizzo di posta elettronica su Internet e poi utilizzarlo per mail pubblicitarie non richieste. Il Garante non può tollerare tali comportamenti intrusivi".

Infatti, ai sensi dell'art. 130 del Codice (riportato nel box) anche un'unica

comunicazione effettuata mediante posta elettronica per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale necessita comunque del preventivo consenso dell'interessato (salvo quanto previsto dal comma 4 del medesimo articolo) e l'eventuale reperibilità di un indirizzo di posta elettronica sulla rete internet non lo rende per ciò stesso liberamente disponibile anche per l'invio di comunicazioni elettroniche non sollecitate.

Il Garante si è espresso poi anche relativamente alla seguente fattispecie: i segnalanti lamentavano la ricezione di pubblicità indesiderata, via telefax, da parte di aziende che promuovevano servizi.

Di fronte all'Autorità, le società hanno dichiarato che i messaggi pubblicitari erano rivolti a soggetti economici presenti negli elenchi "categorici" (es. pagine gialle) e non a consumatori e, quindi, ritenevano di potersi avvalere di una disposizione di carattere generale del Codice della privacy che permette di prescindere dal consenso degli interessati, quando il trattamento riguarda informazioni relative allo svolgimento di attività economiche. Tuttavia, secondo quanto affermato dai segnalanti, i dati personali erano presenti solo su elenchi telefonici ordinari e utilizzabili quindi solo per comunicazioni interpersonali, non avendo fornito alcun consenso per il loro uso a fini di marketing. Né, dalla documentazione è risultato che sia stato richiesto un successivo consenso dei destinatari.

Nel definire tale procedimento, il Garante ha ribadito i principi, più volte affermati, ai quali attenersi per un corretto uso dei dati personali nel settore del marketing telefonico, confermando che è possibile inviare fax o fare telefonate per effettuare ricerche di mercato, promozioni o comunicazioni commerciali, vendite dirette, pubblicità o altro materiale di carattere commerciale solo dopo aver ottenuto il preventivo e esplicito consenso del destinatario.

Ma, se il titolare del trattamento utilizza, a fini di vendita diretta dei propri prodotti o servizi, l'indirizzo e-mail già fornito dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere

il consenso dell'interessato stesso, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso inizialmente o in occasione di successive comunicazioni; però il medesimo interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente capoverso deve essere informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

Le modifiche al testo riportato precedentemente sono state introdotte nell'anno 2009 e recitano quanto segue:

"L'articolo 130 del Codice della Privacy così come modificato dall'art. 20 bis, legge 20.11.2009 n. 166 presenta i nuovi comma 3-ter e 3-quater istitutivi del Registro delle opposizioni che dovrà essere costituito secondo determinati criteri e principi generali come di seguito esposti:

c) previsione che le modalità tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale è intestatario secondo modalità semplificate ed anche in via telematica o telefonica;

e) disciplina delle tempistiche e delle modalità dell'iscrizione al registro, senza distinzione di settore di attività o di categoria merceologica, e del relativo aggiornamento, nonché del correlativo periodo massimo di utilizzabilità dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente;

f) obbligo per i soggetti che effettuano trattamenti di dati per le finalità di cui all'articolo 7, comma 4, lettera b) , di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilità e sulle modalità di iscrizione nel registro per opporsi a futuri contatti;

g) previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli 23 e 24. (Principio opt in affiancato al principio opt out).

3 -quater . La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3 - bis e sul trattamento dei dati sono attribuiti al Garante."

La principale novità introdotta è quindi l'iscrizione al Registro delle opposizioni; (da: http://www.registrodelleopposizioni.it/)[urlh] "Il Registro Pubblico delle Opposizioni è un nuovo servizio concepito a tutela del cittadino, il cui numero è presente negli elenchi telefonici pubblici, che decide di non voler più ricevere telefonate per scopi commerciali o di ricerche di mercato e, in pari tempo, è uno strumento per rendere più competitivo, dinamico e trasparente il mercato tra gli Operatori di marketing telefonico.

Tramite il Registro Pubblico delle Opposizioni si intende raggiungere un corretto equilibrio tra le esigenze dei cittadini che hanno scelto di non ricevere più telefonate commerciali e le esigenze delle imprese che in uno scenario di maggior ordine e trasparenza potranno utilizzare gli strumenti del telemarketing.

Il sistema è chiaro, di facile accessibilità e semplice fruizione.
L'Abbonato può accedere al servizio tramite cinque modalità: modulo elettronico sul sito web, posta elettronica, telefonata, lettera raccomandata, e fax.

L'Operatore potrà iscriversi al sistema e effettuare tutte le operazioni previste per l'aggiornamento delle liste numeriche da contattare attraverso una serie di servizi disponibili sul sito.

La realizzazione e gestione del Registro, istituito con il DPR 178/2010, è stata affidata dal Ministero dello Sviluppo Economico – Dipartimento per le Comunicazioni alla Fondazione Ugo Bordoni attraverso un contratto di servizio che ne sottolinea la natura di ente terzo, indipendente, impegnato in attività di pubblico interesse."

Quindi, in aiuto del cittadino, il registro delle opposizioni offre la funzione di bloccare tutte quelle chiamate indesiderate, che, in mia opinione, risultano spesso "opprimenti", e che possono comportare anche sgradevoli perdite di tempo, o in generale, apportare anche altri tipi di disturbi.

Sempre in mia opinione, il passo successivo che dovrebbe essere compiuto da parte del legislatore, riguarda l'iscrizione al registro anche dei numeri di cellulare, in modo tale da rendere ancora più ampia la libertà del cittadino.

Con l'attivazione del Registro, istituito dal DPR 178/2010, l'Italia è entrata nel regime di opt-out per le telefonate commerciali il quale prevede gli operatori di telemarketing possano telefonare senza bisogno di autorizzazioni a tutti gli utenti non iscritti al Registro pubblico delle opposizioni.

Per informare adeguatamente i cittadini il Garante ha sancito che, alla prima occasione di contatto (stipula di nuovi contratti, fatture, comunicazioni di servizio), le compagnie telefoniche dovranno inviare ai propri utenti un'informativa che illustri le modalità attraverso le quali è possibile registrare il proprio numero telefonico sulla Robinson list[11]: per posta, tramite numero verde, via mail, via fax, direttamente sul sito web.

L'argomento trattato è molto importante perchè sancisce il modo in cui opporsi al telemarketing. Ad oggi è richiesta una chiara e precisa azione da parte degli utenti per manifestare la propria volontà, lasciando così libere le società di operare. In poche parole vige il silenzio assenso inteso come "se non mi dici di no, allora vuole dire che posso chiamare" ossia il opt-out.

Sempre in materia, sarà di competenza del legislatore compiere un ulteriore differenziazione tra telemarketing e mail-marketing, in quanto, a livello personale, risulta di maggior disturbo una comunicazione telefonica che elettronica (in ogni modo vanno entrambe gestite). Inoltre bisogna sempre ricordarsi delle categorie meno capaci in questi ambiti: mi riferisco a persone anziane o , in generale, a coloro i quali non hanno dimestichezza con tali mezzi. Bisognerà mettere nelle migliori condizioni possibili tali soggetti, per poter esprimere con facilità il loro dissenso verso tali mezzi di comunicazione.

In generale è, comunque, buona norma, ogni qualvolta si riceva una simile tipologia di comunicazione, ricordarsi di chiedere come siano riusciti ad arrivare ai nostri dati e al loro trattamento, e inoltre di farsi comunicare numero

[11] Ovvero il registro per le opposizioni del telemarketing

di telefono e nome di chi vi sta chiamando, poiché rientra in pieno nei nostri diritti.

4.4 Lo spamming

Il termine spam trae la sua origine da "Spiced Ham", un particolare tipo di carne in scatola che veniva fornita ai soldati dell'esercito americano e che si guadagnò una fama decisamente negativa; spamming assunse di conseguenza in significato di distribuzione massiccia e continuativa di un qualcosa di non più tollerato. Il termine, usato in senso lato, viene oggigiorno utilizzato per indicare l'invio di comunicazioni elettroniche non richieste ad un lungo elenco di destinatari[12].

Il contenuto dei messaggi elettronici in questione può essere vario. Essi hanno per lo più carattere pubblicitario, ma possono anche avere, ad esempio, finalità di propaganda politica o di proselitismo religioso.

I messaggi di posta elettronica inviati con la tecnica dello spamming sono definiti anche UCE, acronimo di Unsolicited Commercial E-Mail (e-mail non richieste di carattere commerciale).

Nel 2001 la Commissione europea affidò ad una società di consulenza uno studio sul fenomeno dello spamming.

Il risultato dello studio sottolineò come negli USA lo spamming fosse già in declino e come la società americana, sotto la pressione degli utenti di internet, andava dotandosi di strumenti di resistenza all'invasione pubblicitaria nelle caselle di posta elettronica degli utenti; in contemporanea, l'osservazione della situazione americana mise in luce il diffondersi di nuove strategie di marketing via e-mail fondate sul consenso e l'autorizzazione che venivano sviluppate sul mercato mondiale da parte di alcune aziende leader del settore. Queste strategie, decisamente più rispettose della privacy, spostarono

[12]Si veda in proposito, R. Imperiali, codice della privacy: commento alla normativa sulla protezione dei dati personali

la problematica della protezione della vita privata senza darvi una risposta totalmente soddisfacente.

Dal punto di vista europeo, invece, si notò che fino ad allora, le denunce presentate alle autorità nazionali di controllo relative a casi di vero e proprio spamming erano state ben poche e che, più che altro, all'interno dell'Unione europea si discuteva della protezione delle persone e dei loro dati personali in relazione alla ricezione di messaggi pubblicitari elettronici indesiderati; la discussione verteva essenzialmente attorno a due teorie, già viste nei paragrafi precedenti, dell'opt-in e dellìopt-out.

Lo studio del 2001 sottolineò inoltre , come fosse facile confondere lo spamming con la pubblicità indesiderata; si specificò che per spamming s'intende generalmente l'invio massiccio e ripetuto di messaggi pubblicitari non richiesti provenienti da un mittente che maschera o falsifica la propria identità. Pertanto, esso, costituisce evidentemente una forma di comunicazione pubblicitaria non richiesta. Si distingue, tuttavia, anche per il suo carattere massiccio, ripetuto e sleale.

In sostanza, lo spamming è una forma di pubblicità indesiderata, ma non tutte le pubblicità indesiderate sono spamming. In senso stretto una comunicazione pubblicitaria indesiderata presenta due caratteristiche: l'essere pubblicità, ed essere indesiderata, ovvero non richiesta dall'utente.

Negli ultimi anni, con l'emanazione di nuove direttive e il relativo adeguamento delle normative nazionali, la situazione europea, dal punto di vista giuridico-legislativo, è decisamente cambiata e in materia non c'è tutta quella confusione emersa dallo studio precedentemente discusso.

La normativa di riferimento per quanto concerne l'Europa è da riferirsi alla direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002, pubblicata sulla Gazzetta Ufficiale della Comunità Europea L. 201 del 31 luglio 2002, che ha stabilito l'obbligo per gli Stati di legislazioni basate sul principio dell'opt-in, ossia del

preventivo consenso da parte del destinatario.

Per quanto riguarda la scena normativa italiana, lo spam è considerato

già illegale dalla legge 675/96 sulla protezione dei dati personali.

Dopo un periodo di diatriba dottrinale si è affermata la tesi la quale sostenente che, ai sensi dell'art .1 comma 2, lett. c) di detta legge, per dato personale deve intendersi qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Pertanto, è possibile assoggettare a tale disciplina anche l'indirizzo di posta elettronica, come ha ribadito in diverse pronunce il Garante della Privacy.

La giurisprudenza minoritaria ha delineato un'osservazione in merito: non sarebbe possibile parlare di dato personale in senso tecnico nel caso in cui un indirizzo di

posta elettronica non fosse immediatamente ed univocamente riferibile con certezza ad un soggetto .Nella legislazione più specifica nella fattispecie, esiste il decreto legislativo n. 185 del 22 maggio 99, storicamente importante perché schiera l'Italia sul fronte opt-in quando, ancora, le direttive comunitarie non lo imponevano.

Dal punto di vista pratico, invece, se al tempo dello studio l'invio di UCE era conosciuto, oggi, invece, ha raggiunto livelli allarmanti e le ragioni sono facilmente comprensibili: bassi costi della campagna pubblicitaria, alti rendimenti delle attività di marketing e una percentuale più elevata di risposte, rispetto ad altre forme di promozione[13].[Mag05]

Nella minor parte dei casi gli indirizzi e-mail sono forniti da parte degli interessati in modo diretto e molto spesso vengono raccolti in modi occulti dagli spammers, oppure ci si avvale di elenchi preparati e venduti da terzi i quali raccolgono gli indirizzi da spazi pubblici come newsgroup o social network.

In altri casi sono utilizzati programmi, detti generatori casuali, capaci di elaborare in pochissimo tempo miliardi di combinazioni alfanumeriche

[13]Si veda in proposito, M.B. Magro, privacy, ecco la tutela dell'untente on line, in Diritto e Giustizia, 2005

creando automaticamente tutti i possibili indirizzi di posta elettronica di un provider di accesso alla rete.

In altri casi ancora, vengono utilizzati veri e propri motori di ricerca, detti spiders, che cercano indirizzi e-mail in giro per tutta la rete.

Di questi giorni è la notizia degli attacchi da parte di hacker, al sistema della Sony, esattamente dopo la morte del capo dell'organizzazione terroristica Al Qaeda, Osama Bin Laden.

PlayStation Network, PSN, secondo quanto ammesso dagli stessi vertici della Sony sarebbe stata oggetto di un attacco da parte dio alcuni hacker. Pare che 77 milioni di password siano state sottratte insieme ai dati sensibili degli utenti registrati al servizio Playstation Network.

Immediato contraccolpo in borsa dove a Tokyo il titolo Sony scivola perdendo oltre il 4% a causa del timore dei mercati per una possibile class action nei confronti del colosso nipponico da parte degli utenti che hanno subito il furto. Sebbene si tenda a minimizzare sul numero e sull'entità della sottrazione di dati, pare che ci sia il rischio concreto che diversi milioni di italiani utenti registrati di PlayStation Network abbiano subito il furto di nome, indirizzo, e-mail, login, password, oltre che dei dati della carta di credito utilizzata per gli acquisti in rete.

Molti utenti di PSN, allarmati, hanno provveduto a bloccare le proprie carte di credito a titolo precauzionale.

I rischi connessi a questo furto possono essere maggiori di quanto inizialmente si era temuto, infatti qualora gli utenti abbiano usato la stessa password per altre attività, come per il conto, per altre carte etc., la portata dell'attacco degli hacker potrebbe essere decisamente preoccupante. Per costoro, come suggerisce il blog di Playstation, sarebbe preferibile bloccare tutto, farsi sostituire urgentemente le carte e cambiare le password dei servizi online.

Il furto di identità e di dati sensibili in genere e' alquanto diffuso nel mondo anglosassone e nell'Europa continentale, ma ora si sta diffondendo, purtroppo, anche da noi.

L'unica difesa per gli utenti e' quella di usare buon senso e prudenza, come l'accorgimento di verificare sempre le credenziali ed il livello di sicurezza informatica e di protezione dei siti sui quali si effettuano operazioni.

Tornando agli aspetti giuridici, con il parere del 29 maggio 2003[14], il Garante per la protezione dei dati personali, a causa di disagi di numerosi utenti e dei relativi reclami, partendo dal presupposto che "gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia" e che "la loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza consenso libero, specifico e informato", affermò l'illiceità delle mail anonime inviate a scopi promozionali.

A coloro che obbiettarono che gli indirizzi e-mail erano facilmente reperibili in rete, il Garante rispose che questo non comportava di per sé un diritto alla loro utilizzabilità per l'invio di messaggi pubblicitari indesiderati[15].[Cip04]

Per arginare il fenomeno dello spamming, molti provider si avvalgono di sistemi di filtraggio dei messaggi. Ma in generale si possono utilizzare anche altri piccoli accorgimenti, come, per esempio, per un titolare di qualsiasi sito web, alla sezione contatti, sarebbe meglio specificarne i propri nella modalità *mail[at]dominio* piuttosto che *mail@dominio*; questo piccolo accorgimento farà si che i sopracitati motori di ricerca di indirizzi e-mail riconoscano il vostro.

Un ulteriore soluzione, tra le più discusse, per ridurre lo spam in entrata, è quello di introdurre le cosiddette black list, ovvero un elenco di nomi di dominio o indirizzi IP appartenenti a spammers[16].[urli]

Queste liste di indirizzi IP , da cui proviene lo spam, sono state stilate da numerosi soggetti, tra cui ISP, utenti, ed altri ancora, che però non hanno o non avevano nessuna autorizzazione a farlo; per questo motivo , molte volte

[14]Diffuso con un comunicato stampa il 3 settembre 2003

[15]Si legga in proposito, E. Cipolla, le lettere anonime restano illecite anche quando sono elettroniche, in Diritto e giustizia, 2004

[16]Si veda in proposito www.mail-abuse.com

è accaduto che in questi elenchi vengano inseriti anche ISP da cui migliaia di utenti hanno ottenuto un indirizzo di posta elettronica[17].[Cav04] Molto probabilmente per il fatto che alcuni spammers hanno utilizzato account di quel ISP per inviare innumerevoli quantità di spam. La conseguenza di questo sistema fu che il provider venne inserito nelle liste nere come fonte di spamming, ma in realtà esistevano migliaia di utenti con un account su quel provider che non lo erano affatto, e che si videro identificare le proprie mail come spam nonostante fossero di natura legittima.

Tutto quanto finora detto si può trasportare nell'ambito della posta elettronica certificata. Tuttavia bisogna aggiungere altre problematiche di non poca rilevanza; come finora affermato, siamo invasi da SPAM e Phishing[18] provenienti da e-mail reperite in rete con sistemi sempre più sofisticati. Molta colpa è degli utenti che, compilando un modulo on-line non protetto divengono preda di bande organizzate di cracker a causa della trasmissione senza l'ormai comune protocollo SSL.

Il problema si aggrava ora con il sistema PEC poiché la concentrazione degli indirizzi di posta elettronica certificata di tutti i cittadini italiani in pochi server controllati da gestori univoci - o, addirittura, da un solo gestore indicato dal DPCM 06/05/09 in vigore - rende il compito dei cracker non solo più facile, ma estremamente pericoloso in ogni forma attacco sia di tipo 'goliardico' che a carattere delinquenziale.

Cerchiamo ora di fare un quadro sintetico di quanto potrebbe avvenire in tale regime:

1. i cracker avranno una fonte di reperimento e-mail unica al mondo,

[17]Si legga in proposito, G. A. Cavaliere, quale disciplina per i filtri anti-spamming?, 2004

[18]In ambito informatico il phishing ("spillaggio di dati sensibili", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto d'identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

in quanto "certificata" e quindi corrispondente a un titolare che è sicuramente un ente o una persona ben determinata.

2. i cracker avranno una profilazione degli individui, delle imprese e dei professionisti. Ad esempio: tutti gli avvocati iscritti negli albi professionali così come pure tutti gli altri professionisti suddivisi per categoria, oltre che le imprese e gli enti pubblici. In questo modo, potranno inviare messaggi e-mail personalizzati secondo i vari scopi che si prefiggono.

3. i cracker effettueranno furti d'identità avendo la certificazione di base fornita dal sistema PEC. Potranno quindi non solo rubare l'identità di persone, aziende, professionisti ed enti pubblici, ma rivenderanno più facilmente tali dati poiché acquisteranno più valore in quanto entità vere e certificate.

4. i cracker realizzeranno innumerevoli DoS (Denial of Service): attacco che mira a portare il funzionamento di un sistema informatico (Es: un sito web) al limite delle sue prestazioni fino al punto di impedirne l'erogazione del servizio. La limitatezza della capienza delle singole caselle PEC e la loro vulnerabilità non possono, infatti, fermare messaggi in arrivo e questo rappresenta un tiro al bersaglio interessante per tutti coloro che vogliono esercitarsi a riempire anche 1 giga di casella PEC con l'invio di una serie di e-mail con allegati di pesantezza media.

5. i cracker intensificheranno i loro attacchi di pishing: attività illegale utilizzata per ottenere l'accesso a informazioni riservate grazie a messaggi che imitano grafica e logo dei siti istituzionali per ingannare l'utente e portarlo a rivelare dati personali come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc. Avranno, infatti, una marcia in più dal momento che il sito web che mostreranno avrà l'indicazione di una PEC e questo metterà a proprio agio chi vi entrerà fino al punto da indurlo a cliccare sul link poiché si sente più sicuro.

6. i cracker effettueranno Spam Phishing: invio di grandi quantità di

messaggi indesiderati (generalmente commerciali) attraverso qualunque medium allo scopo di frodare il destinatario conducendolo su siti web pericolosi per i loro dati personali. Con gli attuali sistemi, infatti, chi può impedire a un pirata informatico di divenire un cracker certificato (magari cracker@pec.it) e inondare tutto il sistema PEC di qualsiasi cosa?

7. i cracker simuleranno indirizzi PEC. Chi ha detto che non è possibile è qualcuno che non conosce il sistema affatto.

8. L'Art. 34 LEGGE n° 69 del 16 Giugno 2009 ha obbligato a tutta la Pubblica Amministrazione d'inserire il proprio indirizzo PEC nella "Pagina Iniziale" del sito web (obbligo non rispettato da quasi tutta la PA, vedi nostra indagine conoscitiva dove in un campione di oltre 1000 siti della PA solo 25 sono in regola con le disposizioni di legge). Mettere fuori uso e riempire una casella PEC di un a qualsiasi ASL, Comune od altro è un gioco da ragazzi per qualsiasi cracker.

Da quanto finora scritto emerge chiaramente la necessità da parte del legislatore di attuare modifiche al sistema normativo vigente, per rendere l'utilizzo di posta elettronica ancora più sicuro; ma in questo caso, in mia opinione personale, si profila anche la necessità da parte di chi legifera, di affiancarsi a team di sviluppo di sistemi informatici che capiscano le reali necessità degli utenti, al fine di proporre e realizzare sistemi realmente vicini ai cittadini e agli operatori tutti del sistema: con un gruppo di persone con elevate capacità tecniche, unite ad una capacità di intendere comune, ci si può realmente prefiggere gli obbiettivi di una sana informatizzazione.

Capitolo 5

L'informatizzazione della Pubblica Amministrazione

5.1 L'informatizzazione della Pubblica Amministrazione

Già da anni addietro il legislatore italiano si adoperò per favorire, in maniera sempre maggiore, l'impiego delle tecnologie informatiche nella PA per consentire il raggiungimento di obbiettivi quali l'efficacia, l'efficienza e l'economicità delle attività amministrative.

Le nuove tecnologie vengono, perciò, utilizzate, dalle PA, in modo da razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, la modulistica e le modalità di accessi ai servizi da parte dei cittadini e delle imprese.

Il processo di informatizzazione della PA ha avuto luogo a partire dagli anni '90 e, come precisa l'articolo 1 del d.lgsl. n.39/1993, risponde alle finalità di miglioramenti dei servizi, trasparenza dell'azione amministrativa, potenziamento dei supporti conoscitivi per le decisioni pubbliche e contenimento dei costi dell'azione amministrativa.

Con il decreto in esame, e precisamente in base al dettato dell'articolo 4, venne istituita l'Autorità per l'Informatica nella Pubblica Amministrazione

(AIPA), il cui compito fondamentale era quello di promuovere, coordinare, pianificare e controllare lo sviluppo e la gestione dei sistemi informativi automatizzati all'interno delle PA.

Già da anni addietro il legislatore italiano si adoperò per favorire, in maniera sempre maggiore, l'impiego delle tecnologie informatiche nella PA per consentire il raggiungimento di obbiettivi quali l'efficacia, l'efficienza e l'economicità delle attività amministrative.

Le nuove tecnologie vengono, perciò, utilizzate, dalle PA, in modo da razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, la modulistica e le modalità di accessi ai servizi da parte dei cittadini e delle imprese.

Il processo di informatizzazione della PA ha avuto luogo a partire dagli anni '90 e, come precisa l'articolo 1 del d.lgsl. n.39/1993, risponde alle finalità di miglioramenti dei servizi, trasparenza dell'azione amministrativa, potenziamento dei supporti conoscitivi per le decisioni pubbliche e contenimento dei costi dell'azione amministrativa.

Con il decreto in esame, e precisamente in base al dettato dell'articolo 4, venne istituita l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), il cui compito fondamentale era quello di promuovere, coordinare, pianificare e controllare lo sviluppo e la gestione dei sistemi informativi automatizzati all'interno delle PA.

In seguito, con la legge n. 59/1997 (legge Bassanini), che prevedeva all'articolo 15[1] la stipulazione da parte dell'AIPA di contratti-quadro per la fornitura di servizi relativi al trasporto di dati e all'interoperabilità[2], si di-

[1]Si riporta il dettato dell'articolo 15, comma 1, della legge 59/1997:"Al fine della realizzazione della rete unitaria delle pubbliche amministrazioni, l'Autorità per l'informatica nella pubblica amministrazione è incaricata, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, di stipulare, nel rispetto delle vigenti norme in materia di scelta del contraente, uno o più contratti-quadro con cui i prestatori dei servizi e delle forniture relativi al trasporto dei dati e all'interoperabilità si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite"

[2]Con il termine interoperabilità si intende la possibilità di trattamento automatico, da parte di un sistema ricevente, delle informazioni trasmesse da un sistema di proto-

sponeva la realizzazione della RUPA (Rete Unitaria della Pubblica Amministrazione). Questa rete doveva consentire, mediante la trasmissione delle informazioni tra tutte le PA, l'effettiva attuazione del principio dell'accesso del cittadino ai documenti amministrativi e la sua dinamica partecipazione al procedimento[3].[CM05]

La gestione della RUPA fu affidata ad un apposito organismo pubblico denominato Centro Tecnico per la RUPA.

L'articolo 4, comma 2 del d.lgsl. n. 30/1999 aveva, poi, disposto che tutti i Ministeri che si avvalevano di sistemi informativi automatizzati erano tenuti ad assicurarne l'interconnessione con i sistemi analoghi delle altre Amministrazioni Centrali e Locali tramite la RUPA.

Nel 2000 con il d.p.r. n. 445 furono raccolte, in un unico testo, le norme relative alla documentazione amministrativa, tra cui quelle relative al documento informatico e alle firme elettroniche.

Il Piano di azione sull' e-government[4] presentato nel 2000 dal Ministro della Funzione Pubblica delineò la transazione della RUPA ad una rete telematica a copertura nazionale (extranet), che consentisse lo scambio di servizi applicativi paritetici secondo un modello federato, rendendo interoperabili le reti già esistenti sul territorio[5].

Successivamente le "Linee guida del governo per lo sviluppo della società dell'informazione nella legislatura" del 2002, riprendendo sostanzialmente il modello strutturale della rete extranet, prevedevano la realizzazione del Sistema Pubblico di Connettività (SPC), che venne, in seguito, istituito e disciplinato dal d.lgsl. n. 42/2005 e che, doveva assorbire la RUPA entro il

collo mittente, allo scopo di automatizzare anche le attività e i processi amministrativi conseguenti

[3]Si legga in proposito, C Maioli, C. Rabbito, La digitalizzazione della Pubblica Amministrazione, nuove risorse in rete, 2005

[4]Per e-government si intende l'impiego delle tecnologie dell'informazione e della comunicazione, e in particolar modo internet, come strumenti per migliorare la PA

[5]Si legga in proposito, C Maioli, C. Rabbito, La digitalizzazione della Pubblica Amministrazione, nuove risorse in rete, 2005

2007; ci si ritrovava dunque in un periodo di transizione tra RUPA, extranet e SPC.

Sempre nel 2002, per favorire lo sviluppo tecnologico della PA locale, venne pubblicato il Primo Avviso per la selezione di progetti di e-government per i quali vennero destinati alle regioni e agli enti locali circa 120 milioni di euro[6].[urlj]

Il cofinanziamento dei progetti di regioni ed enti locali da parte del Dipartimento per l'Innovazione e le Tecnologie rappresentò l'inizio di una costruttiva cooperazione tra il sistema locale e la PA centrale.

Tra gli obbiettivi che il Primo Avviso si prefiggeva vi era, da un lato, quello di utilizzare le tecnologie informatiche e telematiche per determinare un significativo innalzamento del livello di qualità ed efficienza dei servizi resi ai cittadini e alle imprese; dall'altro, quello di creare, sviluppare e integrare servizi infrastrutturali mediante reti territoriali che consentano l'interconnessione tra le amministrazioni e lo scambio di informazioni e servizi[7].

In particolare, il suo allegato 3, era specificatamente dedicato al protocollo informatico e alla posta elettronica certificata.

Il vantaggio dell'adozione del suddetto protocollo e della gestione dei procedimenti amministrativi in modo elettronico si misurava in aumento sia dell'efficienza interna (attraverso l'eliminazione dei registri cartacei, la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali), e sia di quella esterna, delle amministrazioni verso i cittadini, le imprese e le PA, grazia a strumenti che hanno facilitato l'accesso allo status dei procedimenti e ai relativi documenti e che hanno consentito il monitoraggio della sequenza procedimentale[8].[Lup04]

Al riguardo, il D.P.C.M. Del 14 ottobre 2003 dettò le linee guida per l'adozione del sistema di protocollo informatico e per il trattamento infor-

[6]Si veda in proposito, www.innovazione.gov.it

[7]Si veda in proposito l'articolo 2, comma 2 del Primo Avviso

[8]Si legga in proposito, M. Lupoli, Arriva il "protocollo informatico", cambia la Pubblica Amministrazione, in Diritto e giustizia, 2004

matico dei procedimenti amministrativi; con esso si disposero le condizioni organizzative, funzionali e tecnologiche per la progettazione, la realizzazione e lo sviluppo e la revisione dei sistemi informativi automatizzati al fine di avviare il protocollo informatico[9] e gestire i procedimenti amministrativi in modo elettronico.

Il decreto ribadì l'obbligo per le PA, da assolvere in maniera tempestiva, di definire un piano d'azione dettagliato che dovesse prevedere lo svolgimento di una serie di attività necessarie per l'implementazione del protocollo informatico.

Negli ultimi anni l'uso di tecnologie digitali, introdotte al fine di rinnovare i procedimenti amministrativi, migliorando la qualità del lavoro in termini di tempo ed economicità, ha trasformato profondamente la PA; sia nelle relazioni esterne, sia per quel che riguarda la sua organizzazione interna; per assicurare una diffusione veloce ed omogenea di dati e informazioni tra tutti gli uffici centrali e locali occorre, perciò, garantire l'interconnessione di tutti i sistemi informatici delle PA.

Per facilitare il raggiungimento di tale obbiettivo, uno dei più importanti passi avanti fatti dalle politiche per l'innovazione tecnologica è stato certamente la costituzione del Sistema Pubblico di Connettività (SPC) disciplinato dal d.lgsl. 42/2005.

L'SPC forniva la possibilità di collegare le varie reti centrali, regionali e locali, integrandole in un unico sistema con alti standard di sicurezza, funzionalità e qualità in modo da favorire la comunicazione in rete tra i diversi uffici.

Con il d.lgsl. 82/2005, Codice dell'Amministrazione Digitale, si è resa obbligatoria l'innovazione nella PA offrendo, da una parte, ai cittadini il diritto

[9]Già l'articolo 50 del d.p.r. n. 45/2000 disponeva che le PA provvedessero ad introdurre, nei piani di sviluppo dei sistemi informativi automatizzati, progetti per la realizzazione di sistemi di protocollo informatico; si disponeva inoltre che si predisponessero appositi progetti esecutivi per la sostituzione dei registri di protocollo cartacei con sistemi informatici e che si realizzassero e revisionassero i propri sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico

di interagire sempre, dovunque e verso qualsiasi Amministrazione attraverso internet, posta elettronica e reti; dall'altra, si stabilì che tutte le Amministrazioni dovevano organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale.

Gli effetti del CAD sono stati molteplici: innanzitutto la disciplina giuridica dell'informatica pubblica è stata resa più rigida e gli articoli del d.p.r. n. 445/2000, grazie al loro recepimento all'interno del nuovo testo normativo, diventarono norme primarie; in secondo luogo, il preesistente quadro normativo non venne ridotto poiché il contenuto dei provvedimenti abrogati confluì nell'articolato del nuovo codice; l'ordinamento giuridico non venne razionalizzato, accorpando le disposizioni all'interno di un unico testo[10] e, inoltre, il d.lgsl. 82/2005 interferì con alcuni degli ambiti in cui erano stati prodotti i maggiori sforzi per il riordino dell'ordinamento giuridico[11].[Nat05]

Con il CAD, l'esercizio di tutti i diritti di partecipazione al procedimento amministrativo e di accesso ai documenti amministrativi ha trovato una nuova ed efficace modalità di esplicazione che è stata concretizzata dal definitivo riconoscimento della rilevanza giuridica dell'attività amministrativa resa in forma elettronica[12].[DeG05]

Il codice introdusse nuovi diritti per i cittadini e le imprese e ha definito, inoltre, il quadro giuridico che ne ha garantito l'effettivo godimento.

Tra questi diritti, degni di nota, troviamo: il diritto all'uso delle tecnologie, il diritto all'accesso e all'invio di documenti digitali, il diritto ad effettuare qualsiasi pagamento in forma digitale, il diritto alla qualità del servizio e alla misura della soddisfazione, il diritto alla partecipazione e infine, il diritto a trovare on-line i moduli e i formulari validi e aggiornati.

Con il D.L 185/2008, cosiddetto "Decreto anticrisi", convertito in L.

[10] Ad esempio restarono fuori dal codice dell'amministrazione digitale le norme sul SPC, la disciplina del protocollo informatico

[11] Si legga in proposito, A. Natalini, La semplificazione e la digitalizzazione, Giornale di Diritto Amministrativo, 2005

[12] Si legga in proposito, E. DeGiovanni, Il Codice dell'Amministrazione Digitale:prime impressione, in Diritto dell'Internet, 2005

2/2009, si disponeva all'articolo 16, comma 6, che "Le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali. Entro tre anni dalla data di entrata in vigore del presente decreto tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, comunicano al registro delle imprese l'indirizzo di posta elettronica certificata. L'iscrizione dell'indirizzo di posta elettronica certificata nel registro delle imprese e le sue successive eventuali variazioni sono esenti dall'imposta di bollo e dai diritti di segreteria."

Al comma 7, invece, si legge "I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6 entro un anno dalla data di entrata in vigore del presente decreto. Gli ordini e i collegi pubblicano in un elenco riservato,consultabile in via telematica esclusivamente dalle pubbliche amministrazioni,i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata."

Nel riportare il comma 7 e 6 del decreto anticrisi, ho voluto rafforzare lo sforzo che negli ultimi tempi si sta cercando di compiere per poter accelerare il processo di informatizzazione, attraverso l'obbligo di utilizzo di strumenti elettronici per la comunicazione con le istituzioni pubbliche. La speranza generale è che, oltre al muoversi in ambito legislativo, in maniera consona ed adeguata, ci sia anche un movimento parallelo da parte di chi dovrà poi utilizzare questi strumenti, per fornire un ulteriore accelerata al processo.

In merito a quanto finora scritto, riporto un interessante articolo tratto dal quotidiano "Il Sole 24 Ore", nell'edizione dell' 18 maggio 2011, in cui si parla di ignoranza informatica nelle PA, e dei suoi costi derivanti[urlk]: "Secondo la ricerca, i dipendenti della pubblica amministrazione locale usa-

no il computer per il 69 % del proprio tempo lavorativo, e dichiarano di perdere almeno 47 minuti a settimana dietro alle difficoltà incontrate con lo strumento informatico. Una perdita di tempo attribuibile per un terzo alla scarsa conoscenza informatica, e per il resto ai problemi stessi dei sistemi Ict. Ma quest'improduttività si traduce anche in un costo annuo, per addetto, di circa 1000 euro. Che, confrontato con quello medio di un dipendente della PAL, porta a stimare che il tempo improduttivo speso a causa dell'ignoranza informatica valga circa 346 euro all'anno per dipendente. In totale, più di 205 milioni di euro annui.

«Spesso si pensa che mettere a disposizione strumenti Ict basti a migliorare la performance e la produttività del lavoro, senza porsi il problema di chi li dovrà utilizzare», ha commentato il presidente di Aica, Rodolfo Zich. Così nel tempo «le scarse competenze – spiega Zich - impediscono di sfruttare appieno i vantaggi della tecnologia, se non addirittura creano ostacoli».

Per misurare gli effetti della formazione informatica sulla produttività, sono stati sottoposti a un corso di formazione di base oltre un centinaio di dipendenti pubblici di varie amministrazioni locali. Risultato: conoscenze informatiche cresciute del 23% in termini assoluti e produttività migliorata del 12 per cento.

Il potenziale aumento di produttività nella PAL: 2,2 miliardi di euro l'anno

Poiché si stima che il valore dell'aumento della produttività sia di circa 3900 euro all'anno per ogni soggetto, un piano di formazione su tutti gli utenti informatici potrebbe generare nella PAL un ritorno di ben 2,2 miliardi di euro. Si tratta di stime che, nelle parole del professor Pierfranco Camussone di SDA Bocconi, «devono far riflettere: la PA, nel suo insieme, dà lavoro al 14,6% dei lavoratori italiani». E la PA locale è, per numero di dipendenti, il terzo comparto del settore pubblico dopo l'istruzione e la sanità. «La PA locale – continua Camussone – è il soggetto più vicino a tutti noi, le sue efficienze o inefficienze influenzano la vita quotidiana e le attività delle aziende: la sua capacità di innovarsi con le tecnologie rappresenta un'opportunità per

i cittadini e un volano per le imprese».

Certo non tutte le lentezze sono imputabili all'ignoranza informatica degli utenti: analizzando le chiamate all'help desk in alcuni grandi enti pubblici locali, si è scoperto infatti che, sì, il 40% delle chiamate ha come origine la scarsa perizia informatica del personale, e solo il 17% i guasti nelle infrastrutture. Ma il 26% dei problemi segnalati derivano da errori degli specialisti, che non hanno progettato correttamente l'infrastruttura o ne hanno trascurato l'aggiornamento. Ergo: anche per gli specialisti bisogna prevedere un'adeguata formazione, perché se i problemi nascono a monte, a valle tra gli utenti rischiano di moltiplicarsi.

Un ruolo centrale per l'inclusione digitale del cittadino

Dove la pubblica amministrazione dimostra, in positivo, un ruolo centrale è nei progetti per l'inclusione digitale dei cittadini. Secondo l'indagine di Aica, condotta su oltre 2mila cittadini di quattro regioni che hanno sviluppato un percorso formativo di alfabetizzazione basato sul programma europeo eCitizen (Friuli Venezia Giulia, Emilia Romagna, Lazio, Valle d'Aosta), gli obiettivi di un utilizzo più allargato della rete sono stati raggiunti in pieno. Il 78% dei cittadini a rischio di esclusione digitale, e che hanno partecipato ai corsi di alfabetizzazione, ora usa Internet, contro il 48% relativo all'intera popolazione italiana sopra i 20 anni. E in particolare, contro un 31% riferito ai cittadini appartenenti a categorie socio economiche simili a quelle degli alfabetizzati. Gli scarti principali si sono rilevati per le casalinghe (82% contro un 13% a livello nazionale) e per i pensionati (67% contro un 13%).

«Il fatto che sia la PAL a promuovere le iniziative di e-inclusion – ha osservato Fulvia Sala di Aica – è un valore aggiunto importante, perché gli enti locali hanno quella vicinanza e conoscenza del territorio che permette di creare offerte formative aderenti alla realtà e ai bisogni dei propri cittadini». «Per il futuro – è la conclusione – possiamo solo augurarci che questi interventi si estendano e vengano sostenuti dalle amministrazioni»."

5.2 L'uso della posta elettronica nella Pubblica Amministrazione

Nel maggio 2002, il Consiglio dei Ministri approvava le "Linee guida per lo sviluppo della società dell'informazione nella legislatura" che si ponevano come obbiettivo quello di adottare la posta elettronica per tutte le comunicazioni interne alla PA.

In seguito, nel febbraio 2003, il Centro Tecnico della RUPA, inglobato successivamente nel CNIPA[13], il quale, in base all'articolo 176 del d.lgsl. n.196/2003 ha sostituito l'AIPA, approvava le "Linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata".

Il sistema introdotto era la versione base di uno più recente regolamentato dal d.p.r. n. 68/2005; anche allora erano previste diverse tipologie di ricevute (di accettazione, di avvenuta consegna, di presa in carico); era istituita la figura del gestore (con gli stessi compiti di gestione e conservazione); veniva stilato un elenco di client di posta elettronica compatibili con il sistema e il tutto era disponibile on-line, in una sezione appositamente dedicata del sito web dell'allora Centro Tecnico per la RUPA.

Nel novembre 2003 venne emanata, in seguito, la direttiva del Ministero per l'Innovazione e le Tecnologie in materia di "Impiego della posta elettronica nelle Pubbliche Amministrazioni" col fine di garantire, entro la data della sua scadenza, che tutte le comunicazioni effettuate nelle PA potessero avvenire esclusivamente in via elettronica.

Al paragrafo 2 della direttiva in esame era, poi, disposto che, siccome l'utilizzo della posta elettronica come valido mezzo di trasmissione di documenti informatici era già previsto dall'articolo 14 del d.p.r. n. 445/2000, le PA provvedessero a dotare tutti i dipendenti di una casella di posta elettronica (anche per quelli per i quali non fosse prevista la dotazione di un pc) prevedendo, cosi, la possibilità di richiedere o concedere ferie e permessi, indire riunioni e più in generale inviare comunicazioni di servizio, tramite l'uso

[13]Centro Nazionale per l'Informatica nella Pubblica Amministrazione

della semplice e-mail, confermando l'intento, più volte chiarito in passato dal legislatore, di incrementare l'utilizzo della posta elettronica nella PA.

Inoltre, le PA, dovevano disporre l'attivazione di apposite caselle istituzionali da affidare alla responsabilità delle strutture di competenza, col fine di procedere alla tempestiva lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

Nella direttiva, si leggeva poi, che "la posta elettronica può essere utilizzata per la trasmissione di tutti i tipi di informazioni, documenti e comunicazioni in formato elettronico e, a differenza di altri mezzi tradizionali, offre notevoli vantaggi in termini di maggiore semplicità ed economicità di trasmissione, inoltro e riproduzione; semplicità ed economicità di archiviazione e ricerca; facilità di invio multiplo, ovvero a più destinatari contemporaneamente, con costi estremamente più bassi di quelli di mezzi tradizionali; velocità e asincronia della comunicazione, in quanto non richiede la contemporanea presenza degli interlocutori; possibilità di consultazione ed uso anche da postazioni diverse, anche al di fuori delle postazioni delle Amministrazioni in qualunque momento grazie alla persistenza del messaggio nella sua casella di posta elettronica; integrabilità con altri strumenti di automazione di ufficio, quali rubrica, agenda, lista di distribuzione e applicazioni informatiche in genere."

Il paragrafo 3 della direttiva in esame si occupava, invece, del finanziamento, a favore delle Amministrazioni statali, del progetto @P@, che prevedeva interventi per la diffusione e l'utilizzo degli strumenti telematici in sostituzione dei tradizionali canali di comunicazione. Tale progetto, della cui attuazione era incaricato il CNIPA, prevedeva la realizzazione rispettivamente di: un indirizzo elettronico dei singoli dipendenti (ad uso esclusivamente interno alla PA), caselle di posta elettronica certificata, specifici progetti delle amministrazioni per la trasformazione delle procedure amministrative che utilizzassero il supporto cartaceo in procedure informatizzate e di un Indice,

in cui fossero individuati gli indirizzi istituzionali della PA e l'attribuzione delle corrispondenti caselle di posta elettronica.

L'Indice delle PA veniva gestito dal CNIPA; il costante aggiornamento dei contenuti era condizione indispensabile per l'incremento e il miglioramento dei canali di comunicazione telematica tra le Amministrazioni e tra esse e i cittadini e le imprese. Le informazioni contenute in tali Indice costituivano inoltre prerequisito essenziale per gli obbiettivi di trasparenza e di modernizzazione della PA[14].[urll]

Attraverso l'indice delle PA ogni amministrazione esponeva la struttura dei propri uffici e l'elenco dei servizi offerti, con le informazioni per il loro utilizzo e gli indirizzi di posta elettronica da impiegare per le comunicazioni e per lo scambio di documenti e informazioni, anche ufficiali e a valore legale.

Nell'indice delle PA veniva descritta la struttura organizzativa di ciascuna Amministrazione accreditata, con l'articolazione gerarchica delle varie unità o uffici. Per ciascuna unità venivano resi disponibili gli indirizzi delle caselle PEC attive e di eventuali servizi applicativi resi disponibili on-line.

Esso ha dato inizio, dunque, a un punto di riferimento per l'individuazione e l'accesso alle strutture organizzative e ai servizi telematici offerti dalla PA Centrale o Locale. Inoltre, in esso, venivano pubblicate tutte le informazioni necessarie per lo scambio di messaggi tramite le caselle istituzionali associate ai sistemi di protocollo informatico[15].[urlm]

Tornando al discorso sulla posta elettronica, il CAD del 2005 prevedeva che i cittadini e le imprese che ne facevano richiesta, avevano diritto a ricevere e inviare le comunicazioni da e verso le PA via e-mail all'indirizzo che avevano dichiarato; in questo caso la posta elettronica dalla PA risultava certificata[16]

[14]Si veda in proposito, www.cnipa.gov.it

[15]Si veda in proposito, www.indicepa.gov.it

[16]Si riporta il dettato dell'articolo 6 del d.lgsl. 82/2005: 1. Le pubbliche amministrazioni centrali utilizzano la posta elettronica certificata, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata. 2. Le disposizioni di cui al gomma 1 si applicano anche alle pubbliche amministrazioni regionali e locali salvo che non sia diversamente

e le comunicazioni e i documenti ricevuti in questo modo avevano piena validità giuridica anche attraverso altre persone o aziende.

Con riferimento al CAD attuale, riporto un articolo di G. Rognetta, da www.altalex.com, in cui si parla delle modifiche all'articolo in esame: "Art. 6: utilizzo della posta elettronica certificata Il nuovo comma 1 stabilisce che "Per le comunicazioni di cui all'art. 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata." Allo stato non sono individuabili soggetti che hanno preventivamente dichiarato il proprio indirizzo PEC sulla base della "vigente normativa tecnica"; infatti, la più aggiornata disciplina delle preventive dichiarazioni degli indirizzi PEC non è contenuta in una "normativa tecnica", ma nel D.L. 185/2008 e nel DPCM 6.5.2009. La normativa tecnica è contenuta invece nel DM 2.11.2005, n. 19818, il cui art. 5, riguardante la comunicazione della disponibilità all'uso della PEC, è di fatto inapplicabile, poiché si riferisce alla dichiarazione dell'abrogato art. 4, comma 4, del DPR 68/2005 (abrogazione avvenuta per effetto dell'art. 16, comma 11, del D.L. 185/2008).

Tale inapplicabilità è ribadita dalla circostanza che le comunicazioni di cui all'art. 48, comma 1, cui l'art. 6 rinvia, sono quelle di cui al DPR 68/2005, il cui art. 17 ha condotto appunto alle suddette regole tecniche.

Ora, poiché mancano le nuove regole tecniche di cui all'art. 71, si dovrebbero applicare quelle vigenti, per effetto del combinato disposto dello stesso art. 71, comma 2, e del nuovo art. 6, comma 1, CAD, cioè proprio quelle inapplicabili di cui al DM 2.11.2005: ne deriva un bel pasticcio interpretativo.

Il comma 1 dell'art. 6 così prosegue: "La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano". Anche questa disposizione appare infelice, perché potrebbe interpretarsi come attributiva di una mera facoltà concessa alle pubbliche amministrazioni di utilizzare la PEC, contraddicendo

stabilito.

la stessa "filosofia" del processo di dematerializzazione basato sulla PEC, il cui traino deve essere sostenuto proprio dalle pubbliche amministrazioni. In ogni caso, questa "dichiarazione" si riferisce sempre alla dichiarazione effettuata secondo la predetta evanescente "vigente normativa tecnica". Pertanto, sino a quando non saranno emanate le nuove regole tecniche ai sensi dell'art. 71 CAD, il comma 1 dell'art. 6 CAD rimarrà inapplicabile.

Il comma 1 bis dell'art. 6 dispone che la consultazione degli indirizzi PEC, di cui agli artt. 16, comma 10, e 16 bis, comma 5 del D.L. 185, nonché l'estrazione di elenchi dei suddetti indirizzi da parte delle pubbliche amministrazioni, debba essere effettuata sulla base di regole tecniche emanate da DigitPA.

Questa disposizione blocca la consultazione dei singoli indirizzi PEC e l'utilizzo degli elenchi di PEC e CEC-PAC sino a quando non saranno emanate le regole tecniche da DigitPA; infatti, la precedente normativa non prevedeva l'emanazione di regole tecniche a tal fine. Le emanande regole tecniche, peraltro, se possono avere una giustificazione per la consultazione e l'estrazione degli elenchi di imprese e professionisti, non si comprende quale ruolo possano avere in relazione all'art. 16 bis, comma 5, del D.L. 185, che riguarda le CEC-PAC dei cittadini, per le quali non si pone il problema della consultazione e della estrazione di elenchi, poiché queste dovrebbero avvenire sulla base dei c.d. "indirizzari elettronici" già disciplinati ed esistenti."

Da quanto letto, dunque, si evince la necessità di chiarezza in merito, soprattutto per quanto riguarda l'emanazione delle nuove regole tecniche da parte del CNIPA, per poter far luce, esaustivamente, sulla questione della consultazione degli indirizzi di posta.

L'articolo 47 del d.lgls. n. 82/2005 prevedeva che le comunicazioni tra PA avvenissero "mediante l'utilizzo di posta elettronica", intesa come semplice e-mail, e che esse risultavano "valide ai fini del procedimento amministrativo una volta che ne fosse verificata la provenienza", la quale veniva accertata grazie a strumenti come la firma digitale o altro tipo di firma elettronica qualificata (ovvero tramite l'uso di protocollo informatizzato, ovvero attraverso

i sistemi di posta elettronica certificata).

Il suddetto articolo disponeva, inoltre, che "entro ventiquattro mesi dalla data di entrata in vigore del codice le PA centrali provvedessero a: istituire una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del d.p.r. n. 68/2005 per ciascun registro di protocollo; utilizzare la posta elettronica per le comunicazioni tra le Amministrazioni ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati".

L'articolo in esame nel CAD 2010, con le modifiche apportate con il decreto 235/2011, ha subito le seguenti variazioni: "Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono (...) mediante l'utilizzo della posta elettronica (o in cooperazione applicativa); esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se: a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; b) ovvero sono dotate di (segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445); c) ovvero e' comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71; d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

3. Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. La pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica

o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati."

Le modifiche dunque, sono state apportate solo in merito alla posta elettronica certificata, ovvero laddove si faceva riferimento solo alla posta elettronica semplice, ora trova spazio anche la posta elettronica di tipo certificato, ovviamente sempre nel rispetto delle norme sulla privacy e sul trattamento dei dati personali. Inoltre viene trattato anche l'argomento dell'inserire l'indirizzo nell'indice prima citato; ebbene le modifiche han portato a stabilire che almeno una delle caselle di posta elettronica per ciascun registro di protocollo venga inserita all'interno dell'indice.

L'articolo 48, invece, si è occupato della posta elettronica certificata e disponeva che "la trasmissione telematica di comunicazioni che necessitano di un ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del d.p.r. n. 65/2005".

Tutto ciò nel CAD 2005, che ha visto le seguenti modifiche in quello attuale: "La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

1. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

2. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1."

Si è aggiunta, quindi, l'equivalenza del documento informatico per via

telematica alla notificazione per mezzo di posta, dandogli così maggior valore; inoltre si fa riferimento alla data e all'ora della trasmissione e ricezione di un documento, per poter rendere ancora più efficace il valore probatorio della mail, con tutti i suoi effetti.

5.3 L'E-mail come strumento di notificazione degli atti

Il decreto ministeriale n. 333/1987 ha istituito il servizio pubblico di posta elettronica nazionale (cosiddetto POSTEL); il successivo decreto ministeriale n. 260/1990 ne ha poi disposto il relativo regolamento.

L'invio e la ricezione di messaggi fatti circolare tramite POSTEL venivano garantiti da un sistema di autenticazione, nonché dalla registrazione degli utenti abilitati all'uso di detto servizio, ragion per cui il POSTEL poteva considerarsi correttamente uno strumento valido per le notificazioni[17].[Gio04]

Come più volte ricordato, la legge 59/1997 all'articolo 15, comma 2, ha espressamente previsto che "gli atti, dati e documenti formati dalla Pubblica Amministrazione e da privati con strumenti informatici e telematici[....] nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". Successivamente il d.p.r. 445/2000, all'articolo 14, disponeva che "la trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo di posta nei casi consentiti dalla legge" specificando poi che "il documento informatico trasmesso per via telematica si intende trasmesso e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato".

Tale disposizione venne poi integrata dal d.p.r. n. 123/2001 sul processo civile telematico che introdusse nel nostro ordinamento la possibilità per le

[17]Si legga in proposito, M. De Giorgi, Oggi basta la semplice raccomandata, domani basterà anche l'email, in Diritto e Giustizia, 2004

parti, il giudice e la cancelleria di formare, comunicare, notificare gli atti del procedimento[18] mediante documenti informatici[19].[GR05]

Il d.p.r. 123/2001 ha individuato un sistema informatico di teletrasmissione documentale "chiuso", ovvero non accessibile ad altri elaboratori non autorizzati; venne denominato Sistema Informatico Civile e in base all'articolo 1, lettera f) del regolamento fu definito come "il sottoinsieme delle risorse del dominio di giustizia mediante il quale l'Amministrazione della giustizia tratta il processo civile[20]".[Mel05]

L'articolo 6, inoltre, prevedeva che "le comunicazioni con biglietto di cancelleria, nonché la notificazione degli atti, effettuata quest'ultima come documento informatico sottoscritto con firma digitale, possono essere eseguite per via telematica, oltre che attraverso il sistema informatico civile, anche all'indirizzo elettronico dichiarato ai sensi dell'articolo 7"; quest'ultimo, infatti, disponeva che per poter compiere le comunicazioni e notificazioni suddette, l'indirizzo elettronico del difensore doveva essere esclusivamente quello comunicato dal medesimo al Consiglio dell'Ordine, da questi reso disponibile secondo le regole tecnico-operative; gli esperti e gli ausiliari del giudice facevano riferimento ai propri albi o all'albo dei consulenti presso il tribunale. Per gli altri soggetti l'indirizzo e-mail era quello dichiarato al certificatore della firma digitale, al momento della richiesta di attivazione della procedura di certificazione della medesima, ove reso disponibile dal certificato.

Il terzo comma dell'articolo 7 del d.p.r. n. 123/2001 prevedeva, poi, che gli indirizzi elettronici dei difensori, degli ufficiali giudiziari e degli uffici notifiche, tempestivamente comunicati dagli ordini professionali al Ministero della Giustizia, fossero consultabili anche in via telematica secondo le

[18] Il dettato del d.p.r. n. 123/2001 si applicava al processo civile, al processo amministrativo e a quello dinanzi alle sezioni giurisdizionali della Corte dei Conti

[19] Si legga in proposito, G. Riem, A. Sirotti Gaudenzi, La giustizia telematica e la procedura informatizzata, 2005

[20] Si legga in proposito, M. Melica, L'utilizzo della posta elettronica certificata alla luce delle modifiche al Codice di Procedura Civile: profili operativi, in Diritto dell'Internet, 2005

modalità operative stabilite nel regolamento tecnico del processo telematico.

Con l'emanazione del decreto del Ministero della Giustizia 14 ottobre 2004 si è poi specificato che il sistema del processo di comunicazione e notificazione doveva avvenire attraverso posta elettronica all'interno del sistema del processo telematico su reti protette, grazie all'utilizzo di caselle di posta elettronica certificata per il processo telematico (CPECPT) fornite e gestite dai punti d'accesso, abilitate ricevere messaggi provenienti esclusivamente da altri punti d'accesso e dal gestore centrale[21].

In questo modo gli indirizzi elettronici indicati nell'articolo 7 potevano essere consultati presso il gestore centrale dell'accesso e i punti d'accesso secondo le modalità compatibili con il protocollo LDAP (Lightweight Directory Access Protocol) e si dava la possibilità di effettuare le notificazioni alle parti regolarmente costituite, presso gli indirizzi elettronici dei propri difensori ai sensi dell'articolo 170 c.p.c.

Per ciò che riguarda il momento dell'avvenuta consegna al destinatario delle comunicazioni e notificazioni, l'articolo 8 del d.p.r. n. 123/2001 ha stabilito che "la comunicazione e la notificazione si ha per eseguita alla data apposita dal notificatore alla ricevuta di consegna mediante la procedura di validazione temporale"; per le comunicazioni e le notificazioni eseguite dalla cancelleria e dall'ufficiale giudiziario era sufficiente la data riportata nella ricevuta di consegna e la procedura di validazione temporale non risultava necessaria, in virtù della particolare posizione rivestita da tali soggetti.

Il d.lgls. 82/2005, che come più volte ricordato ha abrogato buona parte del d.p.r. n. 445/2000, ha previsto, all'articolo 48, comma 2, che la "trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta" e al comma successivo ha stabilito che "la data e l'ora di trasmissione e di ricezione di un documento informatico

[21] Ad ogni indirizzo elettronico doveva corrispondere un unica casella di posta elettronica certificata del processo telematico che veniva fornita e gestita dai vari punti d'accesso. La CPECPT poteva ricevere messaggi provenienti esclusivamente da altri punti d'accesso o dal gestore centrale

trasmesso mediante posta elettronica certificata sono opponibili a terzi se conformi alle disposizioni di cui al d.p.r. n. 68/2005, e alle relative regole tecniche".

La legge di conversione del cd. "decreto milleproroghe" (L. n.31/08), del tutto inaspettatamente, ha introdotto (art. 36, commi 2-quater e 2-quinquies) serie modifiche alla disciplina dettata dalla legge 20 novembre 1982, n. 890, recante disciplina in materia di "Notificazioni di atti a mezzo posta e di comunicazioni a mezzo posta connesse con la notificazione di atti giudiziari" (in G.U. 4 dicembre 1982, n. 334).

Viene, in particolare, modificato l'art. 7 della legge citata, che, nella sua attuale stesura, così recita: "1. L'agente postale consegna il piego nelle mani proprie del destinatario, anche se dichiarato fallito.

2. Se la consegna non può essere fatta personalmente al destinatario, il piego è consegnato, nel luogo indicato sulla busta che contiene l'atto da notificare, a persona di famiglia che conviva anche temporaneamente con lui ovvero addetta alla casa ovvero al servizio del destinatario, purché il consegnatario non sia persona manifestamente affetta da malattia mentale o abbia età inferiore a quattordici anni.

3. In mancanza delle persone suindicate, il piego può essere consegnato al portiere dello stabile ovvero a persona che, vincolata da rapporto di lavoro continuativo, è comunque tenuta alla distribuzione della posta al destinatario.

4. L'avviso di ricevimento ed il registro di consegna debbono essere sottoscritti dalla persona alla quale è consegnato il piego e, quando la consegna sia effettuata a persona diversa dal destinatario, la firma deve essere seguita, su entrambi i documenti summenzionati, dalla specificazione della qualità rivestita dal consegnatario, con l'aggiunta, se trattasi di familiare, dell'indicazione di convivente anche se temporaneo.

5. Qualora il consegnatario non sappia firmare o ne sia impossibilitato, l'agente postale fa menzione di tale circostanza sia sul registro di consegna sia sull'avviso di ricevimento, apponendovi la data e la propria sottoscrizione."

Disciplina, questa, che ha superato indenne il vaglio di costituzionalità,

prima con ordinanza n. 210 del 2005 e poi con ordinanza n. 131 del 2007.

La Legge n. 31 del 2008 ha innanzi tutto inserito un comma 6 all'art. 7 che così recita:"*Se il piego non viene consegnato personalmente al destinatario dell'atto, l'agente postale dà notizia al destinatario medesimo dell'avvenuta notificazione dell'atto a mezzo di lettera raccomandata*".

Viene dunque stabilito, a garanzia dell'effettiva conoscenza da parte del destinatario dell'avvenuta notifica, che, qualora l'agente postale provveda alla consegna del piego a soggetto diverso dal destinatario dell'atto da notificare, ha comunque l'obbligo di notiziare quest'ultimo dell'avvenuta notificazione del piego a persona diversa mediante l'invio di una raccomandata al soggetto destinatario.

Senza alcun dubbio, però, la norma di maggior rilievo è quella contenuta all'art. 36, comma 2-quinquies della legge di conversione n. 31 del 2008.

Tale disposizione, infatti, stabilisce che l'obbligo per l'agente postale di notiziare, mediante raccomandata, il destinatario dell'atto dell'avvenuta notifica del piego a terza persona non soltanto "*si applica ai procedimenti di notifica effettuati, ai sensi dell'articolo 7 della citata legge 20 novembre 1982, n. 890, a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto*" ,ma anche che "*Le notificazioni delle sentenze già effettuate, ai sensi dell'articolo 7 della citata legge n. 890 del 1982, alla data di entrata in vigore della legge di conversione del presente decreto non producono la decorrenza del relativo termine di impugnazione se non vi è stata consegna del piego personalmente al destinatario e se è provato che questi non ne ha avuto conoscenza.*"

In base ad una prima lettura della richiamata disposizione, dunque, può affermarsi che il nuovo art. 36, comma 2-quinquies:

a) fa decorrere il nuovo obbligo previsto dall'art. 7, comma 6, della L. n. 890 del 1982 per l'agente postale dal 1° marzo 2008 (l'art. 1, comma 2, della L. 28 febbraio 2008, n. 31, stabilisce infatti che "La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale" e la legge è stata pubblicata sul S.O. alla G.U. n. 51 del 29 febbraio

2008);

b) la notifica della sentenza già eseguita prima dell'entrata in vigore della Legge n. 31 del 2008 (sentenza già notificata al 1° marzo 2008) non produce l'effetto di far decorrere il termine breve per impugnare di cui all'art. 325 cod. proc. civ. (ovvero trenta giorni per proporre appello, revocazione ed opposizione ordinaria di terzo; sessanta giorni per proporre ricorso per cassazione), qualora ricorrano congiuntamente le due condizioni ivi stabilite (l'uso della congiunzione "e" non lascia dubbi in proposito):

1. mancata consegna del piego personalmente al destinatario della notifica

2. prova che il destinatario non ha avuto conoscenza della notificazione del piego (l'onere della quale sembra debba competere al destinatario dell'atto che asserisca di non aver avuto conoscenza della notifica del piego ad uno dei soggetti indicati nell'art. 7).

Per quanto, poi, concerne il riferimento alle "sentenze" contenuto nella norma transitoria, deve tenersi conto della giurisprudenza costante della Suprema Corte secondo cui il termine "sentenza" deve interpretarsi in senso sostanziale di provvedimento definitivo e decisorio, che abbia pronunciato su diritti e status e non sia modificabile e revocabile: deve ritenersi, dunque, che la previsione si applichi anche ai decreti ed alle ordinanze che presentano tali caratteristiche.

Quanto alla portata della disposizione transitoria, riferendosi la norma alle notifiche delle sentenze già effettuate al 1° marzo 2008, la stessa:

a) appare limitata quanto alla disciplina dettata dal codice di procedura civile, tenuto conto della generale previsione di cui all'art. 170 c.p.c., richiamato dall'art. 285, sicché l'effetto sarebbe limitato ai casi previsti dagli artt. 286, comma 2, e 292, ultimo comma, c.p.c. ed ai casi in cui la parte si è costituita personalmente in giudizio ex art. 170, comma 3; mentre, circa la notifica effettuata al procuratore costituito ex art. 170, comma primo, la disposizione potrebbe trovare applicazione per la notifica effettuata a mezzo del servizio postale – è il caso tipico della notifica effettuata a mani della "segretaria di

studio" –, e l'ipotesi assumerebbe rilievo per la vigenza della disciplina "a regime", dandosi luogo ad un ulteriore aggravio delle formalità che rischia di allungare i tempi ed aumentare le incertezze e, probabilmente, aprire anche la strada a nuove declaratorie di incostituzionalità (ad esempio, qualora anche la raccomandata fosse ricevuta da persona diversa dal destinatario, come nel caso della segretaria di studio del procuratore costituito);

b) sembra parimenti limitata, quanto alla disciplina dettata dal codice di procedura penale in tema di notificazioni a mezzo posta (art. 170 c.p.p.), ai soli casi nei quali l'imputato non ha eletto o dichiarato domicilio (applicandosi la speciale disciplina dettata dall'art. 161), ovvero non ha nominato un difensore di fiducia (applicandosi la speciale disciplina dettata dall'art. 157, comma 8-bis, salvo che il difensore di fiducia non abbia dichiarato, contestualmente al deposito della nomina fiduciaria, di non accettare le notificazioni).

Nel caso in cui la notificazione della sentenza al 1° marzo 2008 risultasse eseguita a persona diversa dall'effettivo destinatario, occorre dunque che la parte notificante (pubblica o privata), onde evitare eventuali eccezioni della parte notificata, provveda a reiterare la notifica della sentenza, alla stregua del nuovo obbligo incombente sull'agente postale in base all'art. 7, comma sesto, della Legge n. 890 del 1982.

La limitata portata degli effetti della disposizione transitoria, del resto, trova conferma nel fatto che, se, a seguito della notifica effettuata sotto il regime previgente, il destinatario ha proposto impugnazione, è evidente che lo stesso ha avuto conoscenza dell'atto e non si avrà alcuna conseguenza sul processo.

Diversamente, se il destinatario non ha proposto impugnazione, sembra doversi distinguere: a) se non è ancora decorso il termine di un anno dalla pubblicazione della sentenza di cui all'art. 327 cod. proc. civ., sarà ancora possibile impugnare la sentenza senza alcuna limitazione; b) se, invece, il termine è decorso, la sentenza sarà passata in giudicato, né potrà avere alcun rilievo il fatto che la notifica della sentenza che aveva fatto decorrere il

termine breve sia stata notificata a persona diversa dal destinatario (salvo il caso dell'impugnazione del contumace involontario disciplinato dall'art. 327, comma secondo, cod. proc. Civ.)[22].[urln]

Infine, ribadisco che il 25 gennaio 2011 è entrato in vigore il nuovo codice dell'amministrazione digitale (CAD) come modificato dal D.Lgs n.235/10.

All'art.48 si trova l'equiparazione tra notifica a mezzo posta e trasmissione del documento informatico per via telematica mediante posta elettronica certificata (PEC) salve le sole eccezioni previste dalla legge.

La data e l'ora di trasmissione e di ricezione tramite PEC sono inoltre opponibili ai terzi se effettuate nel rispetto del Dpr 68/2005.

Queste innovazioni vanno lette anche alla luce del D.L. n.185/08 che obbliga imprese, professionisti e pubblica amministrazione a dotarsi di una casella di posta elettronica certificata (PEC) che sarà resa pubblica (es. negli albi professionali e nel registro delle imprese).[G.R11]

Ancora una volta, dunque, da quanto letto, si evincono gli sforzi da parte delle istituzioni nel processo di informatizzazione delle PA; quello di equiparare le notifiche pervenute per mezzo di posta elettronica certificata a quelle pervenute a mezzo di posta tradizionale, è stato sicuramente un decisivo balzo in avanti per l'attuazione di quanto finora auspicato. Restano tuttavia aperte alcune questioni sull'autenticità del mittente, e su alcuni problemi derivanti da questo scoglio; ma tuttavia i passi compiuti possono, opinione personale, ritenersi soddisfacenti, e sarà compito del legislatore, e delle istituzioni, cercare di far chiarezza sulle questioni "spinose".

[22] In proposito si legga la relazione sulla legge n. 31/2008 su www.cortedicassazione.it

Capitolo 6

Aspetti generali

6.1 L'e-government

Il termine e-government si riferisce all'uso delle nuove tecnologie dell'informazione e della comunicazione (ICT) che le pubbliche amministrazioni applicano ad un vasto campo di funzioni amministrative. In particolare, il potenziale networking offerto da internet e dalle sue tecnologie ha il potere di trasformare le strutture e le procedure amministrative.

Il termine inglese e-government deriva da "government", che può significare sia "governo" che "amministrazione", mentre il prefisso "e" sta per "electronic" e viene utilizzato per designare l'insieme delle attività amministrative che si svolgono tramite le tecnologie informatiche e la rete Internet al fine di perseguire gli obiettivi di efficacia, efficienza, economicità, trasparenza e democraticità nell'erogazione dei servizi pubblici e nello svolgimento dei procedimenti amministrativi. La traduzione più fedele di e-government sarebbe pertanto amministrazione elettronica piuttosto che governo elettronico.

L'e-government consiste nell'applicazione delle nuove tecnologie dell'informazione alla causa pubblica con lo scopo di migliorare il rapporto con i cittadini e le imprese:

- Maggiore efficienza
- Maggiore trasparenza

- Maggiore rapidità
- Maggiore adattamento

In questi ultimi anni c'è stata sicuramente attenzione al tema dell'e-Government: si è innanzitutto capito meglio di cosa si tratta, e se ne è allargato lo scopo e la portata. Non solo servizi ed informazioni veicolati tramite Internet a cittadini e imprese: oggi per e-Government si intende un più ampio processo di innovazione della PA, ottenuto grazie al ricorso alle tecnologie ICT, attento alle logiche di funzionamento interno oltre che alle modalità di relazionarsi con l'esterno.

Si è capito soprattutto quale peso dare alle componenti di un progetto di e-Government: se prima la tecnologia era considerata il fattore principale, determinante per il successo di un progetto, oggi le attenzioni si sono spostate altrove. Il fattore fondamentale è quello organizzativo, legato alle modalità di funzionamento delle organizzazioni e soprattutto alle abitudini ed alle aspettative dei cittadini e delle persone che nella Pubblica Amministrazione lavorano. E' un problema innanzitutto di cambiamento culturale che sta avvenendo con lentezza per i molteplici attori coinvolti nel complesso ecosistema dell'e-Government. Nella Pubblica Amministrazione non è ancora immediato proporre innovazione e collaborazione, l'alfabetizzazione informatica della popolazione italiana non è ottimale e le aziende sono generalmente piccole e poco propense all'innovazione di processo. Solo con un più profondo cambiamento di mentalità risulterà più semplice modificare processi e procedure, con l'obiettivo di eliminare attività a scarso valore aggiunto per i funzionari interni e soprattutto per il cittadino.

Questo processo di innovazione non può essere spontaneo, deve in qualche modo essere governato e indirizzato. Nella Pubblica Amministrazione il ruolo della normativa è fondamentale: le leggi possono fare da freno od essere, se chiaramente applicabili, una formidabile spinta all'innovazione ed al cambiamento.

In questi anni, sono proprio gli scogli culturali quelli che si sono affrontati e in parte superati: una costante spinta verso l'alfabetizzazione informatica

e la diffusione di computer all'interno della PA e presso i cittadini, il portare alla ribalta il tema dell'e-Government tramite il meccanismo dei bandi e dei finanziamenti, che ha creato consapevolezza ed interesse nelle PA (soprattutto locali), l'avere alimentato un mercato privato ora consapevole e attento alle esigenze degli Enti.

Dall'altro canto, proprio per questa necessità di creare una spinta culturale diffusa, non sono state fatte scelte di merito estremamente definite, ci si è affidati alla spinta progettuale autonoma degli Enti correndo quindi il rischio di diseconomie e creando differenze nell'applicazione concreta dell'innovazione. Ci si è concentrati soprattutto sui progetti di front-end (servizi al cittadino), perché più semplici e visibili, spesso trascurando di riorganizzare le procedure interne, con alla fine limitati benefici reali per cittadini.

Considerando tutto questo, forse dal punto di vista pratico ancora molto resta da fare, ma senza ombra di dubbio i primi importanti risultati sono stati raggiunti. Lo scoglio più duro, quello culturale, sembra ora decisamente più affrontabile.

A questo punto risulta importante proseguire nella strada intrapresa, rilanciando ulteriormente il tema dell'innovazione della Pubblica Amministrazione italiana mediante la definizione di una strategia di e-Government per l'Italia. Una strategia che non può prescindere dal considerare i numerosi elementi di complessità legati alla concreta attuazione dei cambiamenti richiesti e dal cercare di dare una risposta ai numerosi elementi di criticità che sembrano strutturali nel nostro paese.

L'elemento fondamentale, al di là dei contenuti specifici, sono le modalità con cui questa strategia si deve formare ed attuare, perché sia il più possibile condivisa ed accettata. Da un lato, per permettere di pianificare congiuntamente le iniziative, razionalizzare gli investimenti e contrastare il digital divide, è fondamentale il ruolo di indirizzo e di governo di tipo top-down svolto centralmente.

Dall'altro è importante valorizzare la spinta progettuale, di tipo bottom-up, che favorisca le spinte innovative autonome delle singole Amministrazioni,

più a stretto contatto con i cittadini e i loro bisogni. La strategia deve agire inoltre anche a livello orizzontale, favorendo la collaborazione tra Enti diversi per individuare obiettivi comuni e condivisi e per realizzare iniziative sinergiche.

L'e-government non consiste nella informatizzazione dello Stato che in Italia si può considerare praticamente conclusa[1]. Ma è piuttosto, secondo una definizione dell'Ocse[2], un processo che "migliora l'efficienza, contribuisce alle riforme, aiuta a rafforzare la fiducia tra governi e cittadini e mette alla prova i modi di pensare tradizionali".

La speranza che le nuove tecnologie scatenino un processo spontaneo e duraturo di riorganizzazione della pubblica amministrazione, risolvendo di passaggio anche tutti i suoi problemi storici, non pare purtroppo fondata. L'esperienza internazionale mostra che il successo dell'e-government richiede strategie innovative che, oltre a digitalizzare i dati e mettere online i servizi, puntino a modificare la pubblica amministrazione.

Forse è per questo che nel mondo, secondo uno studio delle Nazioni Unite, tra il 60 e l'80per cento dei progetti di e-government fallisce[3].

Anche se la realtà è certamente molto più complessa, è utile esaminare concisamente due casi estremi e un caso, per così dire, "normale" di e-government.

L'esempio delle radio Vhf per la nautica mostra che automatizzare processi lunghi e involuti può essere superfluo. Per tenere a bordo di un gommone l'indispensabile radio Vhf è necessario il rilascio di un "certificato limitato di radiotelefonista" e di una "licenza di esercizio" da parte del ministero delle Comunicazioni. Dai siti web degli Ispettorati territoriali delle comunicazioni è possibile scaricare i moduli delle domande, ma è una piccola comodità che non migliora l'economia del processo. Il cittadino deve fornire due volte le

[1] Cnipa, Rapporto 2004 sulle attività, pag. 12 (www.cnipa.gov.it).

[2] L'e-Government Project sul sito Ocse (webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf).

[3] UN Department for Economic and Social Affairs, E-Government Readiness Assessment Survey, 2003

stesse informazioni anagrafiche, auto certificare il possesso di "conoscenze e attitudini" relative alla radiotelefonia (un tempo accertate da un esame che però è stato soppresso), effettuare un pagamento di 0,52 euro per la cui riscossione lo Stato spende senz'altro di più, autenticare una foto e allegare una copia del certificato di omologazione della radio, emesso dallo stesso ministero delle Comunicazioni.

Questo processo potrebbe essere automatizzato, ma ne varrebbe realmente la pena? Se il cittadino trovasse nelle confezioni delle radio Vhf una sorta di patente da compilare e rispedire all'Ispettorato rinunceremmo con questo a qualche garanzia fondamentale?

All'estremo opposto, ci sono casi come il fisco telematico, introdotto con la riforma del sistema fiscale italiano del 1997, con i quali l'e-government ha semplificato i processi producendo grandi risparmi[4].[Bar05] I costi di trasformazione sono stati assorbiti nei costi operativi dell'Agenzia delle Entrate, che ha dichiarato risparmi di 90 milioni l'anno di euro stimando inoltre in 200 milioni il risparmio dei contribuenti che inoltrano le dichiarazioni via Internet anziché tramite un consulente fiscale.

È stato necessario intervenire sul fronte normativo (unificazione delle dichiarazioni e dei pagamenti, riduzione del numero delle tasse), organizzativo (accorpamento degli uffici fiscali e riorganizzazione del ministero delle Finanze, creazione dell'Agenzia delle Entrate) e tecnologico (riorganizzazione dei sistemi, servizi online), ma questi interventi impegnativi sono stati realizzati in buona parte all'interno di una singola amministrazione.

In molti altri casi, come quello del protocollo informatico, l'e-government mostra insieme le sue potenzialità e la grande complessità di attuazione. Dieci anni fa, secondo uno studio dell'Aipa, Autorità per l'informatica nella pubblica amministrazione, le attività di protocollazione delle amministrazioni centrali richiedevano 15mila uffici e assorbivano 50mila anni-uomo[5]. Com-

[4]S. Barbuti, The Costs and Benefits of "Fisco Telematico", eGEP 2nd Workshop "Toward a European eGovernment Measurement Framework and Economic Model", Bruxelles, 2005

[5]Aipa, Studio di prefattibilità sul Sistema di gestione dei flussi di documenti (Sistema

plessivamente si stimava una spesa di 20mila miliardi di lire l'anno, cioè 14 miliardi di euro attuali, per svolgere processi che, secondo gli autori dello studio, potevano "essere utilmente collocati tra quelli in cui l'intervento dell'informatica procura i più ampi margini di utilità e, quindi, di miglioramento dei servizi che ci si attende dall'azione amministrativa".

Buona parte degli interventi normativi, tecnologici e anche organizzativi succedutisi negli anni sono dovuti all'Aipa e, dal 2003, al Cnipa, Centro nazionale per l'informatica nella Pubblica amministrazione[6]. Oggi, sulla base dei dati disponibili, gli uffici di protocollo sono diminuiti del 20 per cento e i documenti protocollati in modalità informatica arrivano al 40 per cento del totale[7].[CNI06] Allo stesso tempo, il personale addetto al protocollo sarebbe diminuito solo del 3 per cento mentre le amministrazioni interessate stimano in circa un euro per documento (circa 50-60 di euro milioni l'anno) i costi di realizzazione e gestione del protocollo informatico.

Le ricadute positive della digitalizzazione dei flussi documentali sono innegabili, ma ulteriori interventi di tipo organizzativo, particolarmente da parte delle singole amministrazioni, porterebbero a maggiori benefici. Se il protocollo informatico potesse operare soprattutto su comunicazioni elettroniche le sue potenzialità si realizzerebbero pienamente. Invece, solo il 5-10 per cento dei documenti viaggia via posta elettronica e di questi ben il 64 per cento riguarda scambi informativi interni alla pubblica amministrazione.

Per complicare ulteriormente le cose, nella società dell'informazione si lavora sempre meno con i documenti e sempre più con dati informatici grezzi contenuti nei sistemi informatici di back office[8]. In altre parole, i fatti am-

GEDOC), 1997.

[6] Cfr. il sito del protocollo informatico (protocollo.gov.it) per i dati più recenti e per una rassegna della normativa.

[7] "Protocollo informatico e gestione dei flussi documentali nella Pubblica amministrazione centrale – Stato di attuazione", in I Quaderni Cnipa n° 22, marzo 2006

[8] Con front office e back office si indicano le strutture e i processi di un'organizzazione che si occupano rispettivamente di interagire con gli utenti all'esterno e di gestire le attività all'interno.

ministrativi non sono necessariamente contenuti in fascicoli di carta o in file firmati elettronicamente ma sempre più spesso sono prodotti da elaborazioni su archivi informatici che, per ragioni storiche, ricadono sotto responsabilità eterogenee. Sostituire a un concetto di protocollo incentrato sul documento un altro più adatto a questo contesto richiede approcci e strumenti diversi.

L'e-government contrasta l'arretratezza amministrativa, oggetto in Italia di studi autorevoli, svolti da più parti. Un maggiore coordinamento tra e-government e riforma amministrativa sembra tra gli obiettivi del nuovo esecutivo.

Il "buon andamento" dell'azione amministrativa previsto dall'articolo 97 della Costituzione si dovrebbe tradurre nella capacità di governare i processi amministrativi anche attraverso i sistemi informatici nei quali essi sono ormai materializzati, con lo scopo di creare maggiore valore pubblico[9].[GK02] Dopo il Testo unico sulla documentazione amministrativa e il Codice dell'amministrazione digitale si tratta probabilmente di intervenire ancora sulla semplificazione dei rapporti giuridici tra Stato e cittadini, come pure sull'adeguatezza delle architetture informatiche e sul controllo della qualità dei dati[10].

Lo sforzo compiuto dal legislatore per conservare un aspetto familiare alle rappresentazioni informatiche degli atti amministrativi è considerevole, ma ci si può forse chiedere se abbia ancora un senso adattare il diritto amministrativo all'informatica. Anche per l'e-government, prima di elaborare una politica di settore bisognerebbe rispondere ad una domanda: verso quale modello di pubblica amministrazione deve tendere l'e-government?

Il Piano di e-government 2012 realizzato dal Ministro per la Pubblica Amministrazione e l' Innovazione, definisce un insieme di progetti di innovazione digitale che, nel loro complesso, si propongono di modernizzare, rendere più efficiente e trasparente la Pubblica Amministrazione, migliorare la qualità

[9] G. Kelly, S. Muers, Creating Public Value, Strategy Unit, UK Cabinet Office, 2002.

[10] Cfr. il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Dpr 445/2000) e il Codice dell'amministrazione digitale (decreto legislativo 82/2005).

dei servizi erogati a cittadini e imprese e diminuirne i costi per la collettività, contribuendo a fare della Pubblica Amministrazione un volano di sviluppo dell'economia del Paese.

Il Piano definisce circa 80 progetti, aggregati in 4 ambiti di intervento e 27 obiettivi di Governo da raggiungere entro la legislatura.

Ognuno dei progetti di innovazione previsti dal Piano si propone di produrre dei risultati misurabili ed è scadenzato da rilasci o momenti di verifica intermedi che permettono una pubblica e trasparente valutazione del suo stato di realizzazione.

Gli ambiti di cui prima si parlava sono i seguenti:

- obbiettivi settoriali
- obbiettivi internazionali
- obbiettivi territoriali/di sistema
- progetti speciali

L'area di interesse che riguarda nello specifico la PA è quella degli obbiettivi territoriali/di sistema; per quanto concerne gli obbiettivi territoriali, il lavoro si concentra sul miglioramento dei servizi legati principalmente al sistema anagrafico, cercando di migliorare la raccolta dei dati territoriali, migliorando la carta dei servizi e offrendo servizi ai cittadini in banda larga.

Per quanto riguarda, invece, gli obbiettivi di sistema, questi puntano al miglioramento vero è proprio del rapporto cittadino-pubblica amministrazione; gli obbiettivi di quest'area di interesse sono già stati ampiamente nominati in precedenza (trasparenza ed efficienza della PA, dematerializzazione, sistema pubblico di connettività, rapporto cittadino-PA, trasferimento know-how innovazione, sicurezza dei sistemi informativi e reti), e sono gli elementi fondamentali per la realizzazione di quanto prefisso.

Il piano di azione per l'e-government 2012[11], è stato voluto fondamentalmente per superare il ritardo informatico che ci separa dal resto del nostro

[11] http://www.e2012.gov.it

continente; in Italia, secondo fonti governative, solo il 17% delle famiglie utilizza internet, contro una media europea del 32%; inoltre anche il gap interno non è plausibile, in quanto ci ritroviamo con casi di eccellenza da un lato, ma di grave inefficienza dall'altro, all'interno dello stesso territorio nazionale.

Lo sforzo profuso dal governo in questo ambito, dovrebbe avere anche il merito di migliorare la qualità dei servizi offerti: nello specifico mi riferisco al cosiddetto sistema di trasmissione a banda larga, notoriamente diffuso nei paesi del nord europa, e in quelli del nord America, ma che non sta ancora trovando il meritato spazio nel nostro territorio.

Se si dovesse diffondere pervasivamente l'uso dell'ADSL da parte dei cittadini, occorrerebbe potenziare la rete di trasporto e le dorsali, che altrimenti non sarebbero in grado di sostenere l'incremento di traffico.

E' necessario pertanto un intervento volto al potenziamento della rete nelle aree dove già esiste la maggiore domanda, obiettivo raggiungibile attraverso l'upgrade della rete verso tecnologie NGN.

Sono necessarie operazioni infrastrutturali sugli elementi intermedi delle reti per garantire la fattibilità di interventi sia pur di "minima" quali l'eliminazione del digital divide di prima generazione. Ora, parere personale, la scelta governativa da un lato sembrerebbe anche, da un punto di vista meramente tecnico, giusta, ma, si corre anche in questo caso il rischio di aumentare quel divario già esistente tra zone più abbienti e le zone meno fornite; le scelte andrebbero ponderate bene e bisognerebbe agire in modo da non rendere ancora più marcato questo gap: il piano dovrebbe concedere anche occasioni a tutte quelle zone con meno richieste, facilitando si le prime, ma considerando subito dopo quelle "meno fortunate".

In questa direzione il piano governativo si muoverà cosi[12][urlo]:

1. Chiarezza: al consumatore e alle imprese vanno dichiarati con chiarezza i servizi effettivamente disponibili: se si acquistano 20 mega, ma si dispone effettivamente solo di una parte, occorre fare chiarezza per consentire valutazioni appropriate sia di domanda sia di offerta. Non

[12]Fonte: http://www.e2012.gov.it

ci può essere un politica efficace se il consumatore non conosce il livello effettivo del servizio.

2. Trasparenza: un tavolo con le Regioni deve mappare, insieme agli operatori, l'effettivo svantaggio delle aree marginali che costituirà la road map per gli interventi prioritari contro il digital divide. Le risorse disponibili vanno ordinate secondo queste priorità.

3. De-regolazione: regole semplici e razionali sulla gestione dei sottoservizi urbani riducono tempi e costi della stesura delle reti di nuova generazione nelle aree raggiungibili dagli operatori di mercato. Infatti le opere civili, come scavi, tubature ecc. rappresentano la maggior parte dei costi delle nuove reti (80% circa).

Un interessante quadro della situazione attuale nel nostro Paese ci viene fornito da un articolo tratto da www.pubblicaamministrazione.net: "*I servizi di eGovernment dei paesi europei registrano sensibili miglioramenti, ma esistono differenze anche notevoli fra i diversi paesi. L'Italia si distingue positivamente in alcuni settori, come la sofistificazione dei portali della Pubblica amministrazione dedicati al cittadino e la disponibilità di servizi online. Ma non brilla (pur registrando risultati positivi) in altre voci, come per esempio i servizi business, dedicati alle aziende, ai professionisti, a chi cerca lavoro. Lo rileva il report sull'eGovernment della Commissione Europea elaborato da Capgemini, (attiva nel management consulting, it e otusourcing), Istituto di ricerca Rand Europe, dal Gruppo di analisi IDC e dall Danish Technological Institute (DTI).*

Si tratta della nona misurazione dei servizi digitali delle pubbliche amministrazioni europee effettuata da Bruxelles, e analizza oltre 10mila siti web di 32 paesi (i 27 Ue più Islanda, Norvegia, Svizzera, Croazia e Turchia).

In generale, si riscontrano passi avanti, rispetto al 2009, sul fronte della quantità e della qualità dei servizi al cittadino. Questo fra l'altro, è un settore in cui l'Italia rientra nella top ten.

Nella classifica della disponibilità dei servizi online la Penisola si posiziona addirittura al primo posto, a parimerito con Malta, Austria, Portogallo e Svezia, gli altri paesi che sono al 100% (mentre la media è dell'82%). Buon piazzamento anche nella sofistificazione dei servizi pubblici online, dove raggiungiamo il 99% sia per quelli riservati alle imprese sia per quelli al cittadino.

I punti su cui lavorare maggiormente sono però alcuni servizi definiti "business". Sono ad esempio state fatte comparazioni fra due diversi tipi di servizi: avviare una start up e trovare lavoro. In entrambi i casi l'Italia, pur mantenendosi nella prima metà della classifica, non è fra i paesi in cui il servizio pubblico online è maggiormente completo.

Però proprio in questo segmento il report sottolinea una storia di successo italiana, rappresentata dal portale "Comunica", che da aprile 2010 è diventato l'unico modo per registrare una società.

Sotto la media europeo il livello di accorpamento dei servizi, al 43% contro il 77%. Nel complesso, comunque, l'Italia è perfettamente in media sul fronte dell'usabilità dei servizi e sopra la media per soddisfazione degli utenti.

Il report evidenzia come l'eGovernment sia «al centro di una politica per la riforma amministrativa» con «lo scopo di migliorare l'efficienza e la digitalizzazione». Le best practise italiane: Aia (permesso ambientale integrato), il Processo Telematico (sul fronte della digitalizzazione della giustizia), il sito web dei referti Ulss di Conegliano Veneto (risultati visibili online).

Infine l'eProcurement, un settore in cui il report rileva come l'Europa debba ancora fare passi avanti mentre invece l'Italia eccelle. C'è una piattaforma unica nazionale e il MePa è il primo mercato pubblico lanciato in Europa. L'Italia è fra i paesi che dispongono del maggior numero di piattaforme di eProcurement (fornite anche dalle amministrazioni regionali) ed è sopra la media sia per quanto riguarda il livello nazionale dei servizi sia per quello locale."

6.2 La sicurezza informatica nelle PA

La Sicurezza Informatica può essere definita come l'insieme delle misure di carattere procedurale-organizzativo e tecnologico atte a garantire la Riservatezza, l'Integrità e la Disponibilità delle informazioni e dei servizi, gestiti o erogati, riuniti nell'acronimo RID.

Riservatezza: è la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la visione da parte di soggetti terzi non autorizzate. La riservatezza risulta necessaria per la trasmissione dei dati sensibili ed è dunque uno dei requisiti che garantiscono il rispetto della vita privata degli utenti. Le informazioni sono un bene (asset) che deve essere protetto da minacce specifiche, al fine di garantire la continuità del servizio e minimizzare le eventuali perdite di dati. Rientra in questo ambito la problematica dell'autenticazione sicura ovvero dell'identificazione certa ed univoca del soggetto che accede al sistema ed ai dati.

Integrità: è la veridicità che i dati trasmessi, ricevuti o conservati siano completi e non alterati. Il requisito dell'integrità dei dati è significativamente importante rispetto alle procedure di conclusione dei contratti o quando è indispensabile garantire l'accuratezza dei dati stessi come nel caso di dati medici, dati relativi alla progettazione industriale, ecc.

Disponibilità: è l'esigenza che i dati siano sempre accessibili e che i servizi funzionino anche nel caso di interruzioni dovute, ad esempio, alla cessazione dell'energia elettrica, a eventi disastrosi naturali, eventi imprevisti e/o ad attacchi di pirateria informatica. È un requisito di primaria importanza nei casi in cui l'indisponibilità di una rete di comunicazione può generare disfunzioni rispetto all'erogazione del servizio.

Per ognuno di questi tre ambiti sarà necessario attuare una serie di procedure e misure specifiche, al fine di costituire un Sistema di Gestione della Sicurezza Informatica da applicare alla PA nelle sue molteplici e diverse articolazioni. I fattori contribuenti alla necessità di un SGSI sono essenzialmente la necessità di protezione dei beni (asset) e le debolezze della tecnologia (intrinseche e non). I suoi elementi costitutivi sono invece individuabili nell'area

tecnologica, in quella organizzativa e in quella legale.

Va da sé che maggiore è il valore che si assegna al bene da proteggere (asset) maggiore dovrà essere lo sforzo, anche finanziario, che dovrà essere compiuto per la protezione del bene medesimo. I Sistemi di Gestione per l'Information Security (detti anche Information Security Management Systems, o "ISMS") hanno come obiettivo principale l'implementazione di adeguati controlli, sotto forma di strutture organizzative, policy operative, istruzioni, procedure e funzioni software, atti ad assicurare il soddisfacimento di specifici obiettivi di sicurezza stabiliti dall'ente.

Sovente si tende ad identificare il termine riferito alla sicurezza informatica con le norme relative alla privacy di cui al D.L.vo 193/2006 che rappresentano invece uno specifico aspetto della più complessa problematica. Oggi, rispetto al passato, con la crescita dell'uso di nuove tecnologie come i dispositivi portatili, la virtualizzazione dei sistemi operativi, la banda larga e le connessioni flat, le reti Wireless (Wi-Fi, Wi-Max e Bluetooth), nonché con l'introduzione sempre più diffusa delle tecnologie RFID e VoIP e dei software per il file sharing e quanto altro ancora "vive" nel panorama delle ICT la battaglia per la protezione dei dati assume un rilievo tale che non ci si può più affidare a soluzioni "fai da te".

La sicurezza delle informazioni è quindi un insieme di misure ad ampio respiro finalizzato da una parte a proteggere le informazioni elettroniche per mezzo della sicurezza informatica e dall'altra a proteggere le informazioni cartacee attraverso misure organizzative.

A livello europeo lo standard BS 7799:1 (British Standard Institute) prende in considerazione l'intero processo di gestione delle informazioni e prevede il coinvolgimento e l'integrazione di tutti gli elementi della catena del valore dell'impresa, ovvero le persone, i processi, le tecnologie, al fine di consentire una corretta gestione delle informazioni e ridurre il rischio di danneggiamenti, furti, accessi non autorizzati. La BS 7799:1 è recepita nella normativa ISO 17799 del 1995.

Alla BS 7799:1 si affianca la BS 7799:2 che recentemente è stato pub-

blicata come ISO 27001 ed è certificabile, mentre l'ISO 17799 viene definito come manuale pratico (Security Code of Practice) privo di valore normativo, ovvero una delle tante metodologie adottabili per soddisfare i requisiti della norma ISO 27001. Tale norma introduce il concetto di "Sistema di Gestione", uno strumento che permette di tenere sotto controllo in modo sistematico e continuativo tutti i processi legati alla sicurezza delle informazioni tramite la definizione di ruoli, responsabilità e procedure formali sia per l'operatività aziendale, che per la gestione delle emergenze.

In Italia, per la Pubblica Amministrazione, il 16 Gennaio 2003, il Ministero per l'Innovazione Tecnologica, d'intesa con il Ministero delle Comunicazioni hanno rilasciato la c.d. "Direttiva Stanca per la PA" in cui sono descritte le Best Practice. Tali procedure fanno esplicito riferimento alla norma BS in questione. Gli Standard sono un presupposto di valore in quanto:

Definiscono degli importanti elementi di garanzia anche contrattuali, interpretabili come "livelli di servizio", oppure come specifiche organizzative condivise tra le parti.

Definiscono la macro-struttura organizzativa per l'implementazione, il controllo e per il miglioramento continuo per definiti aspetti del sistema di gestione.

Introducono l'auditing interno, quale processo per il monitoraggio della presenza e dell'efficacia dei controlli, nonché in considerazione della necessità della pianificazione delle attività di miglioramento

Definiscono le condizioni per una corretta gestione dei diversi rischi, compresi quelli di natura ambientale, tra i quali quelli relativi alla sicurezza delle informazioni.

Ciascun ente dovrebbe disporre di un "Sistema di Gestione della Sicurezza delle Informazioni", ed osservare il modello processuale definito dal BS che propone la metodologia - di derivazione del processo di controllo di qualità ancorché applicata in maniera più stringente e severa – Plan, Do, Check, Act (Pianificare, Eseguire, Verificare, Mantenere) per un'analisi dei rischi e la successiva predisposizione del documento programmatico della sicurezza e

del documento per la gestione degli incidenti.

La rappresentazione schematica in quattro settori circolari ideata da Edwards Deming, che nel 1946 introdusse in Giappone il controllo di qualità.

FASE 1: PLAN – Pianificazione e scelta del SGSI. La fase di Plan consiste nell'identificare il problema, nell'analizzarlo, nell'individuare le cause reali, nel definire e pianificare le azioni correttive. Obiettivi della pianificazione sono:

1. Razionalizzare gli interventi
2. Condividere gli obiettivi
3. Condividere i processi
4. Mantenere traccia del processo decisionale
5. Disporre di uno strumento per verificare il raggiungimento degli obiettivi
6. Predisporre i piani finanziari

FASE 2: DO – Implementazione del SGSI. La fase di Do consiste nel preparare e applicare le azioni pianificate, a livello di test.
FASE 3: CHECK – Monitoraggio e revisione del SGSI. La fase di Check consiste nel verificare i risultati delle azioni intraprese, confrontandoli con gli obiettivi attesi.
FASE 4: ACT – Mantenimento e miglioramento del SGSI. La fase di Act consiste nello standardizzare e consolidare se il check è stato positivo, introducendo le modifiche nel ciclo produttivo, oppure nel preparare un nuovo ciclo PDCA se il check ha rilevato nuovi inconvenienti. Il tema della sicurezza informatica viene letto nel Codice dell'Amministrazione Digitale sotto profili diversi, anche se interconnessi tra loro. Innanzitutto sotto il profilo della sicurezza dei sistemi informativi e dei dati della pubblica amministrazione e, quindi, delle regole di sicurezza del sistema pubblico di connettività. Poi sotto il profilo della tutela della riservatezza delle informazioni e, quindi,

della tutela della privacy. Il terzo profilo, infine, non strettamente attinente alla pubblica amministrazione, si riferisce più in generale alla sicurezza del documento informatico e della firma digitale.

La sicurezza nei sistemi informativi è senza dubbio un tema di forte interesse, poiché, come si può evincere da quanto finora scritto, la dipendenza delle organizzazioni dalle reti e dai sistemi informatici è un fattore di rilevanza fondamentale. Introdurla all'interno delle Pubbliche Amministrazioni significa evitare l'esposizione dei sistemi ad eventi distruttivi, e ridurne l'eventuale impatto sul sistema aziendale.

Fino ad oggi ci sono state sporadiche e parziali iniziative, magari non accompagnate da una reale evoluzione dei processi interni; in un certo senso si è seguiti un inerzia organizzativa che ha prodotto una domanda disaggregata in termini di requisiti funzionali e piattaforme di riferimento. Lo sbaglio commesso in generale è il vedere la sicurezza come un costo, piuttosto che un opportunità.

Senza ombra di dubbio, si può affermare che un buon livello di sicurezza nei sistemi informativi permette una buona riuscita di tutti gli elementi costituenti l'e-government e l'e-governance; il moderno ambiente distribuito, base delle forme governative citate, introduce nuove vulnerabilità relative alla sicurezza delle reti: da una parte, la possibile intercettazione di password e di dati, dall'altra, la modifica dei dati stessi.

A questi problemi, inoltre, bisogna aggiungere la crescita continua della popolazione di utenti potenziali, i netizen[13], con i relativi problemi connessi alla loro identificazione sui server, che rende quindi la sicurezza a livello fisico non più sufficiente.

Per quanto riguarda le esigenze dei database distribuiti, che costituiscono la base delle reti distribuite, si può affermare che questi presentano le stesse funzionalità e gli stessi meccanismi di sicurezza delle reti distribuite: si basano su sistemi di identificazione e autenticazione, applicano politiche

[13]Per netizen, acronimo di "citizen" e "net", si intendono gli utenti che utilizzano il mondo del web

di controlli degli accessi, implementano processi di audit e accountability e sfruttano tecniche di cifratura delle reti; tutto questo fornice una garanzia di fiducia su questi sistemi.

Soltanto una metodologia completa, accurata e in accordo con gli standard in vigore può consentire di raggiungere gli obbiettivi di sicurezza e garantirla cosi in un ambiente distribuito; questa metodologia deve essere pubblica, ovvero reperibile direttamente dall'azienda; non deve essere segreta o proprietaria (mi soffermerò in maniera approfondita sull'argomento più avanti) in quanto questo precluderebbe l possibilità di ottenere la futura certificazione di sicurezza.

È necessario per le PA avviare il cosiddetto "progetto sicurezza""; il progetto è costituito da varie entità che rendono completa la protezione dei sistemi:

- bisogna adottare uno standard di riferimento per tutte le PA (mancante allo stato dell'arte!)
- bisogna definire lo scenario da proteggere
- bisogna individuare le minacce pertinenti (fisiche, logiche, organizzative)
- bisogna instaurare meccanismi di sicurezza in grado di attuare le funzioni di sicurezza
- bisogna dotarsi di "device" già pronti o da realizzare necessari per attuare i meccanismi di sicurezza (le contromisure)
- bisogna stabilire degli obbiettivi di sicurezza da raggiungere ("ensure")

Le funzioni di sicurezza atte a garantire la protezione di un sistema devono essere in accordo con ITSEC.

La valutazione della sicurezza dei sistemi e prodotti informatici è un'operazione molto complessa poiché, per essere significativa, deve tener conto

di una variegata gamma di elementi sia interni che esterni al sistema o prodotto considerato. Nell'approccio al problema della sicurezza informatica è sempre tenere presente che non basta progettare un sistema avente sofisticati meccanismi di protezione se questo sarà successivamente utilizzato da personale, non sufficientemente sensibilizzato ai problemi di sicurezza, che lascia incustoditi dischetti e tabulati contenenti informazioni riservate. Occorrerà tenere presente anche la variabile "umana" e valutare in che modo essa incide sul sistema.

In generale le misure di sicurezza possono essere suddivise nelle seguenti due categorie:

- misure di sicurezza tecniche, realizzate da meccanismi hardware, firmware o software;
- misure di sicurezza non tecniche, di tipo fisico, procedurale o sul personale.

I criteri ITSEC affrontano principalmente il problema della valutazione delle misure di sicurezza tecniche, ma considerano anche specifici aspetti non tecnici nel caso in cui questi siano necessari per il corretto funzionamento delle misure tecniche. Dal campo di applicabilità dei criteri sono esplicitamente esclusi alcuni aspetti (perché generalmente sono oggetto di normative specifiche) come ad esempio: il controllo delle emissioni elettromagnetiche, l'uso di contenitori resistenti all'effrazione, la qualità degli algoritmi e dei protocolli crittografici. In particolare, con riferimento ai meccanismi crittografici, i criteri richiedono esplicitamente che questi siano certificati da un apposito organismo costituito in ogni Paese.

I criteri ITSEC hanno come obiettivo la valutazione sia di sistemi che di prodotti informatici. Secondo la terminologia ITSEC, un sistema informatico è un apparato utilizzato per scopi ben specificati in un ambiente operativo completamente definito; un prodotto informatico, invece, è un pacchetto software o un dispositivo hardware progettato per l'uso e l'installazione in una grande varietà di sistemi. Poiché un sistema è progettato per soddisfare i

requisiti di un particolare gruppo di utenti finali e di un particolare ambiente operativo, lo studio dei relativi problemi di sicurezza può essere effettuato con riferimento alle reali condizioni di impiego. Al contrario chi progetta un prodotto può solamente cercare di soddisfare esigenze di sicurezza di tipo generico, non conoscendo a priori l'ambiente in cui esso verrà utilizzato. Malgrado queste differenze ITSEC prevede che sistemi e prodotti siano valutati secondo gli stessi criteri.

In ITSEC, l'oggetto dell'analisi è detto obiettivo di valutazione, mentre la persona o l'ente che richiede la valutazione è detto sponsor. La valutazione di un sistema viene effettuata in relazione all'obiettivo di sicurezza che è un documento costituito dai seguenti quattro elementi:

1. una cosiddetta politica di sicurezza del sistema (che è denominata System Security Policy) nel caso sia in discussione la valutazione di un sistema o una definizione delle caratteristiche funzionali del prodotto (che si chiama tecnicamente Product Rationale) nel caso oggetto della analisi di sicurezza siano i prodotti informatici;

   (a) una specifica delle funzioni di sicurezza che permettono il conseguimento degli obiettivi individuati;

2. il livello minimo dichiarato di robustezza dei meccanismi (in termine tecnico strength of mechanisms);

3. il livello di valutazione che si desidera conseguire.

Esiste poi un ulteriore elemento, che può essere discrezionalmente proposto dallo sponsor, costituito dalla definizione dei meccanismi di sicurezza richiesti.

L'individuazione del livello di sicurezza viene definita esclusivamente dallo sponsor. il quale identificati gli obiettivi di sicurezza del sistema sulla base dell'analisi dei requisiti operativi del sistema o del prodotto, dell'ambiente operativo reale (nel caso dei sistemi) o presunto (nel caso dei prodotti) per il quale il livello di sicurezza è pensato e delle minacce alla sicurezza (reali o

presunte). All'identificazione degli obiettivi di sicurezza contribuiscono, inoltre, gli aspetti legali e ogni altro regolamento particolare, come ad esempio l'eventuale politica di sicurezza dell'ente nell'ambito del quale la valutazione dovrà essere eseguita. Gli obiettivi così identificati permettono di individuare le funzioni di sicurezza che l'operazione di valutazione deve fornire e di stabilire il livello di fiducia in tali funzioni più adeguato al contesto delineatosi nel corso delle analisi.

Nel caso dei sistemi, le minacce e gli obiettivi di sicurezza concorrono alla definizione della cosiddetta system security policy definita come l'insieme delle leggi regole e pratiche che stabiliscono come le informazioni e le risorse critiche per la sicurezza devono essere gestite, protette e distribuite all'interno del sistema. La system security policy deve coprire tutti gli aspetti di sicurezza del sistema incluse le misure di sicurezza di tipo fisico, procedurale e sul personale.

Vale la pena precisare in modo esplicito che i processi che portano all'identificazione delle minacce e degli obiettivi di sicurezza e in definitiva alla costruzione di un security target , non sono oggetto di valutazione; in altre parole stabilire se un determinato security target è adeguato alle specifiche esigenze di sicurezza dello sponsor non è, secondo l'approccio ITSEC, compito del valutatore.

Peraltro è necessario evidenziare che i criteri ITSEC definiscono tre diversi stili di specifica che lo sponsor deve utilizzare nella stesura della documentazione: informale, semi-formale e formale. Una specifica informale è scritta in linguaggio naturale, una specifica semi-formale richiede l'uso di una notazione ristretta in accordo con un insieme di convenzioni predefinite e infine una specifica formale è scritta tramite una notazione fondata su rigorosi principi matematici.

Va infine ricordato che i criteri ITSEC hanno per oggetto la valutazione tanto dei sistemi quanto dei prodotti informatici.

Le funzioni di sicurezza devono dunque rispettare:

- integrità

- riservatezza
- disponibilità

I meccanismi di sicurezza sono in grado di attuare le funzioni di sicurezza sia a livello hardware, a livello software e sia per le comunicazioni; tutto questo grazie al relativo controllo delle macchine, degli accessi logici o della sicurezza delle linee.

I sistemi di sicurezza invece devono essere scelti in base ad una politica di riferimento: questa è un documento vitale per le organizzazioni e deriva dalla necessita di proteggere i dati e di attuare procedure interne ed esterne alle organizzazioni. In accordo con la politica di riferimento si possono realizzare livelli di sicurezza centralizzati o distribuiti: questo dipende dalle scelte dei responsabili e dei punti di gestione. Infine va ricordato che una buona metodologia aiuta a scrivere la politica di sicurezza, durante l'attuazione della stessa.

Come prima accennato, sposto ora l'attenzione sul mondo del software open source all'interno della PA.

I programmi "Open Source Software" letteralmente traducibile in "sorgente aperta" definizione spesso abbreviata in "OSS"), sono utilizzabili in via del tutto analoga ai programmi a codice chiuso, ovvero al software proprietario, tanto che, spesso, non è ravvisabile alcuna significativa differenza operativa tra il software OSS e quello CSS ("Closed Source Software", ovvero a "sorgente chiusa"). La differenza tra le due categorie è costituita, pertanto, non dalla utilizzabilità in sé ma dalle facoltà connesse all'utilizzo concesse dall'autore mediante la specifica licenza OSS, mentre la licenza del software proprietario, limita in vario modo le facoltà di utilizzare o di copiare il programma, la licenza OSS conferisce, infatti, all'utilizzatore una serie di facoltà estremamente ampie. Una sintetica definizione di "Open Source Software", può essere formulata, pertanto, come "software" (ovvero "programma" per computer, applicazione, sistema operativo, ecc) in cui l'autore abbia stabilito di concedere una serie di fondamentali libertà all'utilizzatore attraverso un

"license agreement", tra le quali vi sono la possibilità di studiare il funzionamento del programma, di adattare il codice sorgente alle proprie esigenze, di aggiornare il programma, di utilizzarlo per ogni scopo e su qualsiasi numero di macchine e di redistribuire copie del programma ad altri utilizzatori.

Nell'ambito dell'Unione Europea sono state varate iniziative specifiche per la promozione e diffusione delle risorse informatiche a codice aperto sia nel settore pubblico che nel mondo imprenditoriale privato. La Commissione Europea ha predisposto un programma denominato IDABC ovvero "Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens", finalizzato all'utilizzo delle opportunità offerte dalle tecnologie della comunicazione e dell'informazione, di fornire consulenza e sostegno per i servizi del settore pubblico nei confronti dei cittadini e delle imprese in Europa, nonché di migliorare l'efficienza e la collaborazione fra le pubbliche amministrazioni europee. L'esigenza di maggiore interoperabilità, di maggiore sicurezza e di redditività sta determinando un interesse crescente fra le pubbliche amministrazioni dell'Unione Europea sull'uso del software a codice aperto, effettivamente, OSS ha parecchie caratteristiche che soddisfano le necessità delle gestioni del settore pubblico. Permette che le organizzazioni ripartiscano il software e lo riutilizzino per sviluppare le soluzioni adattate ai loro bisogni, assicura l'utilizzo di standard aperti, così migliorando l'interscambio e la parità d'accesso alle informazioni ed ai servizi del settore pubblico. Quindi, la Commissione Europea ha assunto una linea propositiva nei confronti degli Stati Membri nella direzione dell'open source nell'ambito del proprio programma generale di armonizzazione delle procedure gestionali nel settore pubblico.

Nel sistema giuridico italiano, nel giugno 2002, con il documento ufficiale dal Ministro per l'Innovazione e le Tecnologie intitolato "Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura" è stata introdotta la definizione nominale di "open source", in particolare, al capitolo 1.2 si riporta la seguente considerazione: "Si diffonderanno gli standard aperti e i software open source, cioè i software liberi, la cui proprietà

non sia di un singolo fornitore ma governati da una licenza d'uso che ne garantisce la possibilità di libero utilizzo, scambio, studio e modificabilità."

All'Open Source era interamente dedicato il paragrafo 8.9 che si riporta: "Va fatta un'approfondita valutazione, in linea con quanto sta facendo l'Unione Europea, sulla strategia open source per la Pubblica Amministrazione. I prodotti open source (per caratteristiche intrinseche derivanti dalle stesse modalità di sviluppo e di evoluzione) determinano vantaggi 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) In qualità di semplice utilizzatore, la Pubblica Amministrazione può quindi immediatamente rivolgersi al mercato dei prodotti open source per ridurre in modo consistente e rapido i costi di acquisizione e gestione di molte applicazioni software. Questo è vero per le piattaforme per servizi web, per gli ambienti operativi dai personal computer ai sistemi centrali, a molti strumenti di produttività individuale. Inoltre, in qualità di catalizzatore, per la dimensione della domanda che rappresenta e per la possibilità di aggregare e supportare piccole realtà di sviluppo e ricerca, creando la necessaria massa critica, la Pubblica Amministrazione può avvantaggiarsi del modello open source in vari modi, tra i quali lo sviluppo di infrastrutture software per la connettività multicanale, lo sviluppo di piattaforme di interoperabilità, di soluzioni specifiche per la Pubblica Amministrazione e di piattaforme strategiche per il Paese (ad esempio quelle di eLearning ed eHealth)."

In data 19 dicembre 2003 il Ministro per l'Innovazione e le Tecnologie ha emanato una Direttiva "Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni." il cui contenuto è stato, poi, posto a fondamento di alcune disposizioni contenute nel Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale". In tale Direttiva il Ministro per l'Innovazione espressamente prevedeva, all'art.3 che "1. Le pubbliche amministrazioni, nel rispetto della legge 7 agosto 1990, n. 241 e del decreto legislativo 12 febbraio 1993, n. 39, acquisiscono programmi

informatici a seguito di una valutazione comparativa tra le diverse soluzioni disponibili sul mercato. 2. In particolare, valutano la rispondenza alle proprie esigenze di ciascuna delle seguenti soluzioni tecniche: a) sviluppo di programmi informatici ad hoc, sulla scorta dei requisiti indicati dalla stessa amministrazione committente; b) riuso di programmi informatici sviluppati ad hoc per altre amministrazioni; c) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso; d) acquisizione di programmi informatici a codice sorgente aperto; e) acquisizione mediante combinazione delle modalità' di cui alle lettere precedenti.". All'art. 4 la Direttiva prevede, inoltre, che "Le pubbliche amministrazioni, nella predisposizione o nell'acquisizione dei programmi informatici, privilegiano le soluzioni che presentino le seguenti caratteristiche: a) soluzioni informatiche che, basandosi su formati dei dati e interfacce aperte e standard, assicurino l'interoperabilità' e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione, salvo che ricorrano peculiari ed eccezionali esigenze di sicurezza e segreto; b) soluzioni informatiche che, in assenza di specifiche ragioni contrarie, rendano i sistemi informatici non dipendenti da un unico fornitore o da un'unica tecnologia proprietaria; la dipendenza e' valutata tenendo conto dell'intera soluzione; c) soluzioni informatiche che, con il preventivo assenso del C.N.I.P.A. ed in assenza di specifiche ragioni contrarie, garantiscano la disponibilità' del codice sorgente per ispezione e tracciabilita' da parte delle pubbliche amministrazioni, ferma la non modificabilità' del codice, fatti salvi i diritti di proprietà' intellettuale del fornitore e fermo l'obbligo dell'amministrazione di garantire segretezza o riservatezza; d) programmi informatici che esportino dati e documenti in più' formati, di cui almeno uno di tipo aperto.". Ruolo fondamentale per la promozione di tale direttiva è attribuito al Centro Nazionale per l'Informatica nella Pubblica Amministrazione (C.N.I.P.A.).

Il CNIPA ha l'obiettivo primario di dare supporto alla pubblica amministrazione nell'utilizzo efficace dell'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa. Il ruolo del CNIPA

dello specifico ambito dell'Open Source è particolarmente incisivo, come è testimoniato dall'inserimento, nel Piano Triennale per l'Informatica 2006-2009, di uno specifico paragrafo, il 3.9, intitolato "La diffusione del software open source". In attuazione della Direttiva del Ministro per l'innovazione e le tecnologie del 19 dicembre 2003 (G.U. 7 febbraio 2004, n. 31), il CNIPA ha costituito l'Osservatorio Open Source, avente lo scopo di monitorare le iniziative poste in essere della Pubbliche Amministrazioni, analogamente a quanto avviene in ambito europeo presso l'Open Source Observatory . Nell'ambito dell'Osservatorio è attiva la pagina dedicata alla "Rilevazione continua sull'uso del software Open Source nella PA italiana" all'interno della quale è possibile accedere alle schede informative delle soluzioni adottate dalle varie amministrazioni. L'attuale disciplina normativa è costituita dall'art. 68 e seguenti del Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (pubblicato nella Gazzetta Ufficiale n. 112 del 16 maggio 2005 - Supplemento Ordinario n. 93), il cui testo, in gran parte trae, origine dalla Direttiva del 19/12/2003 già menzionata. Si rivela l'intento, da parte del legislatore, del concetto di "non dipendenza da un unico fornitore" nonché di "disponibilità e tranciabilità del codice sorgente", ovvero di due elementi fondamentali della "filosofia" open source. In ogni caso nell'art. 68 del D. Lgs. 82/2005 si prevede un obbligo da parte delle pubbliche amministrazioni, di procedere ad una "valutazione comparativa di tipo tecnico ed economico" tra una serie di soluzioni specificamente indicate: a) sviluppo di programmi informatici per conto e a spese dell'amministrazione sulla scorta dei requisiti indicati dalla stessa amministrazione committente; riuso di programmi informatici sviluppati per conto e a spese della medesima o di altre amministrazioni; b) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso; c) acquisizione di programmi informatici a codice sorgente aperto.

Si rammenta, che la soluzione relativa ai programmi proprietari, essendo posta al punto b) della elencazione, dovrebbe intendersi come sovraordinata rispetto a quella relativa ai programmi proprietari posta al punto c), per-

tanto, il ricorso ai programmi open source sia inteso dal legislatore soltanto come soluzione "di riserva" subordinata alla intervenuta impossibilità di ottenere il programma richiesto mediante soluzioni di tipo proprietario. Così come impostato, sembrerebbe obiettivo del tutto residuale e non, invece, di obiettivo primario, come avrebbe dovuto essere posto secondo le indicazioni provenienti dalle Istituzioni Comunitarie, vi sono, tuttavia, altri elementi che devono essere valutati per verificare l'allineamento del legislatore alle indicazioni comunitarie, come viene offerto dallo stesso art. 68 il cui secondo comma prevede espressamente la natura aperta a livello di dati (non di programmi, pertanto, per i quali vale il primo comma dell'art. 68) affermando che nella rappresentazione dei dati e documenti in più formati uno debba essere "di tipo aperto, salvo che ricorrano peculiari ed eccezionali esigenze", ovvero, come stabilito dal terzo comma, "un formato dati reso pubblico e documentato esaustivamente". Il rovesciamento delle graduatoria preferenziale presente nel testo dell'art. 68
del D. Lgs 82/2005 viene, tuttavia, espressamente previsto, dall'art. 1, comma 892 e 895 della L. 27 dicembre 2006 n. 296 (legge finanziaria 2007). Al comma 892 viene autorizzata una spesa di 10 milioni di euro all'anno - per tre anni - a sostegno dei progetti per la Società dell'Informazione. In riferimento a tali progetti il comma 895 prevede che sia data priorità a quelli che utilizzano e/o sviluppano applicazioni a codice sorgente aperto per la Pubblica Amministrazione. Viene, pertanto, testualmente formulata una chiara presa di posizione del legislatore a favore del codice aperto, più di quanto fosse emerso nella precedente normativa.

Il Ministro per le Riforme e le Innovazioni nella P.A., presso la Presidenza del Consiglio dei Ministri, ha, infine, pubblicato, nel mese di marzo 2007, un documento denominato "VERSO IL SISTEMA NAZIONALE DI E- GOVERNMENT - LINEE STRATEGICHE" in cui viene ampiamente ribadito l'atteggiamento nei confronti delle risorse open source, deve notarsi che tra i sette obiettivi espressamente indicati nel predetto documento viene dedicato all'open source il sesto, così testualmente conformato: "Creare un

ambiente favorevole alla competitività delle imprese e dare impulso alla crescita dell'industria ICT, promuovendo un ruolo di "procurement strategico" da parte della PA, un innalzamento della qualità della domanda di tecnologie e servizi innovativi, incrementando la diffusione e la utilizzazione di soluzioni Open Source.". La Presidenza del Consiglio dei Ministri, per il tramite del Dipartimento per l'Innovazione e le Tecnologie, risulta, pertanto, avere concretamente intrapreso la via indicata dalla Commissione Europea anche in riferimento all'adozione degli strumenti informatici con caratteristiche di tipo aperto.
La fonte ufficiale per avere informazioni sulle concrete implementazioni di progetti e programmi open source è costituita dal sito web "Osservatorio Open Source" del CNIPA[14][urlp], da dove si evince che "La rilevanza internazionale assunta dal fenomeno ha indotto il MIT a promuovere uno studio sul software a codice sorgente aperto al fine di consentire una corretta valutazione delle possibilità d'utilizzo nella PA. La distribuzione ed evoluzione del software OS può infatti determinare una serie di vantaggi in termini di contenimento dei prezzi, trasparenza e sicurezza, non dipendenza da un unico fornitore, elevata riusabilità, accessibilità per le piccole realtà di sviluppo." Dalla lettura delle schede sono riscontrabili le più varie implementazioni presso pubbliche amministrazioni ed enti pubblici, tra le varie schede si ritiene opportuno porre in evidenza le realizzazione sotto Linux effettuata dalla Presidenza del Consiglio dei Ministri nel progetto "e-urop@" avente come oggetto la realizzazione di un "portale di raccolta di documentazione dei processi normativi europei e diffusione con inoltro ufficiale del Ministro per le Politiche Comunitarie verso organi istituzionali, regioni e autonomie locali per la partecipazione alla fase ascendente del processo creazione delle norme europee".

Altra esperienza di rilievo è quella realizzata dal Ministero della Giustizia avente come oggetto la "gestione informatizzata dei giustificativi (fe-

[14]Da: http://www.osspa.cnipa.it/home/

rie,malattie, permessi, ecc.) del personale della Direzione Generale dei sistemi informativi automatizzati.". Molto interessante, soprattutto per gli strumenti informatici utilizzati, è la procedura implementata dal Ministero degli Affari Esteri denominato "Rete Mondiali Visti" in cui risultano coinvolti Apache, Firefox, Linux e OpenOffice. Anche il sito istituzionale dell'ISTAT è stato realizzato con strumenti open source, quali il server Apache, un sistema operativo su kernel Linux, ed il data base MySQL.

Il CNR ha realizzato un Progettazione e sviluppo di un sistema per la gestione contabile dell'Ente con Eclispe e Linux.
I sistemi operativi open source hanno trovato concreta applicazione nell'ambito dell'implementazione tecnologica del Processo Telematico e, quindi, nell'ambito del Sistema Informatico Civile predisposto dal Ministero della Giustizia. In particolare, come si può leggere sia nel documento "Regole Tecnico-Operative per l'uso di strumenti informatici e telematici nel processo civile", sia nel documento "Specifiche di Interfaccia tra Punto di Accesso e Gestore Centrale", Versione 2.0 predisposto dal Ministero della Giustizia al punto 5.1: "Per il progetto del Processo Telematico si è adottato Linux come sistema operativo dei sistemi server, e quindi anche per PolisWeb presso il Punto di Accesso è consigliata l'adozione di Linux.". Pertanto tale espressa menzione del sistema operativo open source per eccellenza costituisce, una concreta applicazione di soluzioni open source dal lato server.

L'Open source ormai ha la strada spianata verso un meritato successo. Meritato nella misura in cui pone l'essere umano al centro di una percorso tecnologico che riabilita il concetto di libertà come "veste" naturale della persona stessa. Un diritto che non si dovrebbe negare, il libero arbitrio appartiene a ciascuno di noi.

L'open source sta diventando protagonista in diversi Paesi del mondo. I dati che girano sono infiniti e le esigenze di sicurezza per controllarli e tutelarli crescono su base esponenziale. Avere il codice sorgente aperto nei programmi utilizzati all'interno della propria organizzazione, significa che i controlli atti a ricercare eventuali debolezze del sistema, o blackdoor, sono

più agevoli (nel software proprietario ci si deve rivolgere al produttore).

La presunta assenza di finalità commerciali per quanto riguarda i canoni di licenza e la necessità di fornire il software con il codice, per consentire di adattarlo alle realtà locali prima di distribuirlo e ridistribuirlo, condurrebbero naturalmente ad aderire al modello Open Source.

Un'altra convinzione è che i vantaggi in termini economici saranno immensi e che tale risparmio consentirà maggiori, e migliori, investimenti per potenziare i servizi pubblici in rete e per promuovere l'alfabetizzazione informatica dei cittadini.

Un pensiero è d'obbligo esprimerlo: un prossimo futuro, Internet e l'impiego di strumenti informatici diverranno una costante di vita per quasi tutti noi, per lo studio, per il lavoro, per i contatti sociali..., dunque è davvero opportuno che in ogni computer non sia installato soltanto software prodotto da una sola azienda.

Attualmente, la tesi a favore della leadership di quest'ultima, non è ancora confutata.

Capitolo 7

Conclusioni

Una Pubblica Amministrazione efficiente e trasparente deve necessariamente poter contare su una efficace comunicazione istituzionale interna ed esterna. Per fare ciò deve realizzare una nuova struttura organizzativa che, basata sulle nuove tecnologie informatiche, consenta di interagire in maniera sicura e veloce con l'utenza garantendo ad essa l'esercizio della cittadinanza attiva.

Le difficoltà da superare per realizzare tali strutture tecnologiche sono molte e tra queste vi è anche il digital divide che, in tutte le sue varianti, rimane una tra i maggiori fattori che maggiormente determinano la lentezza dell'adeguamento degli uffici pubblici alle nuove esigenze organizzative imposte dai tempi e dalle normative più recenti.

Il primo tipo di divario digitale in cui la pubblica amministrazione si è imbattuta è stato quello relativo alla compatibilità tra i diversi sistemi informatici in uso presso le sue numerose ramificazioni. Essa, talvolta, non riguardava solo i sistemi tra amministrazioni diverse ma anche quelli utilizzati all'interno della stessa struttura.

Con il tempo, con le nuove strutture informatiche e, soprattutto, attraverso la tecnologia sviluppatasi attorno ad internet, molti di questi divari sono stati superati altri, però, se se ne sono aggiunti rallentando, quando non anche bloccando, il difficile processo di modernizzazione della PA.

All'interno delle numerose ed articolate strutture dell'amministrazione pubblica, si possono facilmente individuare tutte le tipologie di divario digitale :

- mancanza di strumenti informatici
- incompatibilità tra sistemi informatici diversi
- tipo di accesso
- competenza nell'uso degli strumenti

E' chiaro che, in presenza di tali e tanti tipi di divario digitale, il processo di ristrutturazione degli apparati della P.A. procede in maniera estremamente lenta e differenziata.

Spesso ci si trova di fronte a strutture, come quella citata del Comune di Bologna, che sono all'avanguardia in Europa, altrettanto spesso però, ci si trova di fronte a situazione diametralmente opposte.

Le cause di tutto ciò sono molteplici. Una, però, sembra prevalere su tutte le altre. Come succede molto frequentemente in Italia, le migliori intenzioni che il legislatore esprime attraverso ottime norme, vengono vanificate dall'assenza in esse di sanzioni da applicare in caso di inadempienze. Un esempio: il DPR 445 del 2000, il decreto del Ministro per l'Innovazione e le Tecnologie del 14/10/2003 ed il D.Lgs. 82/2005 impongono l'adozione del protocollo informatico ed il trattamento informatico dei procedimenti amministrativi a tutti gli uffici pubblici. Risulta, invece, che molti Uffici, e sicuramente la grandissima parte dei Comuni, si è limitata all'adozione del protocollo informatico, trascurando il trattamento digitalizzato dei suddetti procedimenti. Per la verità, alcuni comuni non hanno attivato, o non utilizzano appieno, neanche il protocollo informatico. A questo bisogna aggiungere che nella struttura organizzativa e nelle piante organiche dei comuni di medie e piccole dimensioni, spesso non è stato neanche previsto l'ufficio Sistemi Informatici, né la figura del responsabile informatico. Con tali inadempienze e senza che alcun organismo intervenga per far rispettare le norme che esistono, il

digital divide che viene a crearsi tra le diverse strutture della P.A., nonché all'interno delle stesse strutture, non potrà che aumentare e compromettere seriamente il processo di evoluzione e ristrutturazione degli uffici pubblici che è base fondamentale per la realizzazione di una comunicazione istituzionale efficace ed aperta alla cittadinanza.

Allo stato attuale si può affermare che il più delle volte, anche a causa del divario digitale, l'organizzazione burocratica tende ancora ad adattare i nuovi strumenti informatici alla struttura esistente anziché, come sarebbe auspicabile, il contrario.

Si può, inoltre, affermare che l'introduzione di un codice dell'amministrazione digitale ha introdotto nuove problematiche: si è creata un'amministrazione digitale fai-da-te, con disorientamento tra gli operatori, con alcune soluzioni organizzative affrettate e con principi di efficacia dell'azione amministrativa che in ambiente digitale faticano ad essere compresi, se non di rado sacrificati in nome dell'efficienza e dell'applicazione formalistica di una norma che meriterebbe ben altra sorte.

Si tratta di un indubbio effetto placebo, perché le continue modifiche e il persistere dell'assenza di regole tecniche portano inevitabilmente al differimento della sua applicazione concreta, come in realtà è avvenuto.

Infatti, l'instabilità del quadro normativo provoca in chi deve applicarlo o farlo applicare una disaffezione che scaturisce dall'inaffidabilità intrinseca. A riprova, basti pensare al solo fatto che anche il quadro sulle firme elettroniche è mutato sei volte in poco più di dieci anni.

In buona sostanza, non si può ingabbiare l'informatica in una norma, ma anzi, proprio in adesione al principio comunitario della neutralità della norma rispetto alla tecnologia, si rende necessaria una norma di principio generalista e mai generica. Infatti, come è stato ampiamente dimostrato negli ultimi anni dai provvedimenti sulla conservazione sostitutiva, da AIPA prima e da CNIPA poi, appena una norma "tecnologica" viene pubblicata in Gazzetta ufficiale diviene di conseguenza già vecchia e superata dalla tecnologia stessa, che avanza a una velocità di anni luce superiore a quella del legislatore.

Qualora continuassimo in questo accanimento normativo, saremmo di fronte a un insieme magmatico di norme sempre più stratificatesi nel tempo e che risentirebbe, per forza di cose e indipendentemente dalla volontà del legislatore, di una mancanza di una visione globale e sincronica dell'amministrazione digitale.

Non servono più, dunque, nuove rivisitazioni del Codice, nonostante qualche ritocco indispensabile, ma il varo di norme tecniche e applicative. Queste ultime non dovranno essere calate dall'alto, ma riviste insieme agli operatori del settore, a chi si occupa di diritto dell'informatica e di informatica giuridica, di archivistica e di diplomatica, di informatica generale e di diritto nel senso più ampio. Né va dimenticato il ruolo delle associazioni che permettono con i loro contributi di far attecchire le nuove tecnologie nelle amministrazioni pubbliche e che in questi anni hanno svolto un ruolo determinante per la disseminazione dell'amministrazione digitale applicata con rigore metodologico.

L'uso delle tecnologie digitali è ormai imprescindibile per il professionista. Il lavoro è profondamente cambiato in seguito alla diffusione su larga scala di computer, internet e software professionali, tutti strumenti che consentono di accelerare le procedure, con apprezzabili guadagni di produttività.

La trasformazione in atto ha reso necessario un adeguamento e, per molti aspetti, un ripensamento del quadro normativo. Il processo di adeguamento normativo è stato particolarmente problematico a causa della rapidità dell'informatizzazione delle attività professionali, e della novità delle soluzioni tecniche da tradurre in schemi giuridici.

Per alcuni anni si è verificato uno scollamento, fortemente sentito dai professionisti, tra le possibilità offerte dalle nuove tecnologie e il riconoscimento di certezza e validità giuridica ai nuovi strumenti digitali.

Da ciò l'incredibile attività del nostro legislatore che per risolvere questi evidenti problemi di adeguamento ha cercato di disciplinare l'introduzione di nuove tecnologie in maniera troppo dettagliata con un approccio di carattere tecnicistico che mal si concilia con quelle naturali caratteristiche di generalità

ed astrattezza delle disposizioni legislative.

Contrastate ed in parte vanificate da una serie di controtendenze, palesi e occulte, queste varie e pur meritevoli iniziative legislative hanno però conseguito finora esiti poco apprezzabili, rendendo indispensabili nuovi e complessi interventi normativi e organizzativi che non sempre riescono nell'intento di migliorare e consolidare il quadro giuridico dell'innovazione.

In effetti l'avverarsi della "società globale dell'informazione", con l'universalità e l'interoperabilità delle infrastrutture e dei servizi, rende del tutto inadeguati gli approcci settoriali via via seguiti nell'affrontare il tema "informatica e pubblica amministrazione" e impone una visione d'insieme delle varie problematiche giuridiche ad esso attinenti e delle loro reciproche relazioni.

Ma a questo punto ci si domanda: perché il legislatore non riesce a disciplinare in maniera organica ed esauriente e principalmente con pochi provvedimenti le nuove tecnologie? Perché si persevera nel seguire questa fallimentare politica legislativa?

Indubbiamente non può essere sottaciuta l'enorme difficoltà di accostamento ad una materia come le nuove tecnologie che spesso impone un totale cambiamento di mentalità e quindi il doppio sforzo di considerare gli inevitabili risvolti giuridici ed organizzativi legati all'introduzione di un nuovo strumento.

Ad esempio nel mondo "tangibile" della carta scritta, è la sottoscrizione autografa apposta dal privato in calce al documento che esprime sino a prova contraria il consenso del firmatario sul contenuto dell'atto sottoscritto, per quanto riguarda invece il documento informatico, per attribuire con certezza lo stesso al suo autore si fa ricorso alla cd. firma elettronica che utilizza gli strumenti della moderna crittografia.

Ma al di là di questa ineccepibile premessa esistono tanti altri elementi che testimoniano un approccio non proprio ideale del legislatore nel mondo ICT.

Le motivazioni sono molteplici: talune riconducibili ad aspetti di caratte-

re normativo, altre a problematiche di carattere tecnico-organizzativo, altre ancora a questioni di carattere economico.

Il mio lavoro inizialmente intendeva mostrare i principali strumenti di comunicazione utilizzati dalle pubbliche amministrazioni per lo scambio di dati; nel mostrare quelli più frequentemente adottati, ho cercato di far emergere anche il quadro normativo che li regolamenta, ma soprattutto ho cercato di dare un continuo storico di tale quadro, cercando di capire da cosa è nato, ma soprattutto come si è evoluto, per definire uno scenario chiaro e attuale.

Nel definirlo, però, è emerso un dato lampante: in un certo qual modo è possibile affermare che la giurisdizione sta "inseguendo" la tecnologia.

Le continue modifiche del CAD apportate negli ultimi 6 anni, dal 2005 ad oggi, sono il segno di quanto finora detto.

Un altro dato che però è emerso, è la non piena imputabilità del legislatore riguardante la questione: noto è il fatto che la tecnologia si sviluppa con una rapidità tale da rendere difficile il lavoro di chi deve legiferare su di essa. Auspicabili in questo senso, dovrebbero essere snellimenti nei tempi e nei modi di emanare leggi in merito, grazie anche agli strumenti che sono stati elencati in quanto finora scritto.

Bibliografia

[Bar05] S. Barbuti. *The Cost and Benefits of Fisco Telematico.* eGep workshop, 2005.

[Cam03] M. Cammarata. *Privacy su internet: gli indirizzi e-mail non sono pubblici.* interlex.it, 2003.

[Cav04] G.A. Cavaliere. *Quale disciplina per i filtri anti spamming?* 2004.

[CC05] G. Sartor C. Cevenini, C. Di Cocco. *Lezioni di informatica giuridica.* GEdit, 2005.

[Cev02] C. Cevenini. *Il documento informatico e la firma digitale.* Clueb, 2002.

[Cip04] E. Cipolla. *Le lettere anonime restano illecite anche quando sono elettroniche.* Diritto e Giustizia, 2004.

[CM05] C. Rabbito C. Maioli. *La digitalizzazione della Pubblica Amministrazione.* 2005.

[CNI06] CNIPA. *Protocollo informatico e gestione dei flussi documentali nella Pubblica Amministrazione centrale-Stato d'attuazione.* I quaderni CNIPA, 2006.

[CNI10] CNIPA. *La posta elettronica certificata.* CNIPA, 2010.

[DeG05] E. DeGiovanni. *Il Codice dell'amministrazione digitale:prime impressioni.* Diritto dell'Internet, 2005.

[Fab] N. Fabiano. *La posta elettronica certificata:qual'è la reale portata giuridca?* Altalex.com.

[Fil02] C. Filippi. *La centralità dell'informazione e della conoscenza per il funzionamento dei sitemi economici: il problema della "società della classificazione".* 2002.

[Fin] G. Finocchiaro. *Diritto di Internet.* Zanichelli.

[Fin03] G. Finocchiaro. *Firma digitale e firme elettroniche: profili privatistici.* Giuffrè, 2003.

[GC04] S. Fadda G. Cassano. *Codice in materia di dati personali:commento articolo per articolo al Testo Unico sulla privacy.* Ipsoa, 2004.

[Gia00] A. Giannaccari. *La crittografia come strumento per garantire la riservatezza delle comunicazioni.* Rivista Diritto Informatico, 2000.

[Gio04] M. De Giorgi. *Oggi basta la semplice raccomandata, domani basterà anche l'e-mail.* Diritto e Giustizia, 2004.

[Giu09] C. Giustozzi. *Privacy:le raffiche di fine anno.* interlex.it, 2009.

[GK02] S. Muers G. Kelly. *Creating public value strategy unit.* UK Cabinet Office, 2002.

[GR05] A. Siroti Gaudenzi G. Riem. *La giustizia telematica e la procedura informatizzata.* 2005.

[G.R11] G.Rognetta. *Il nuovo CAD: un intralcio per la posta elettronica certificata?* altalex.com, 2011.

[Imp04] R. Imperiali. *Codice della privacy: commento alla normativa sulla protezione dei dati personali.* il sole 24 ore, 2004.

[Jor05] G.M. Jori. *L'efficacia probatoria dell'e-mail.* Giurisprudenza Italiana, 2005.

[Leo] F. Leotta. *Internet e le nuove frontiere di tutela della privacy.* diritto.it.

[Lis04] A. Lisi. *L'e-mail è forma scritta?* altalex.com, 2004.

[Lon] T. De Longo. *La pec gratuita ai cittadini non è un invenzione di Brunetta.*

[Lup04] M. Lupoli. *Arriva il protocollo informatico, cambia la Pubblica Amministrazione.* Diritto e Giustizia, 2004.

[Mag05] M. B. Magro. *Privacy, ecco la tutela dell'utente on line.* Diritto e Giustizia, 2005.

[Mai02] C. Maioli. *E-Governance ed E-Government.* Clueb, 2002.

[MC04] E. Maccarone M. Cammarata. *Un messaggio e-mail non è prova scritta.* interlex.it, 2004.

[Mel05] M. Melica. *L'utilizzo della posta elettronica certificata alla luce delle modifiche al codice di procedura civile:profili operativi.* Diritto dell'Internet, 2005.

[Nat05] A. Natalini. *La semplificazione e la digitalizzazione.* Giornale di diritto amministrativo, 2005.

[Rog99] G. Rognetta. *La firma digitale e il documento informatico.* 1999.

[urla] http://www.microsoft.com/,.

[urlb] http://www.digitpa.gov.it/,.

[urlc] http://www.PAdigitale.it/,.

[urld] http://www.saperi.forumpa.it/,.

[urle] http://www.blogstudiolegalefinocchiaro.it/,.

[urlf] http://www.fnada.it/,.

[urlg] http://www.garanteprivacy.it/,.

[urlh] http://www.registrodelleopposizioni.it/,.

[urli] http://www.mail-abuse.com/,.

[urlj] http://www.innovazionepa.gov.it/,.

[urlk] http://www.ilsole24ore.com/,.

[urll] http://www.cnipa.gov.it/,.

[urlm] http://www.indicepa.gov.it/,.

[urln] http://www.cortedicassazione.it/,.

[urlo] http://www.e2012.gov.it/,.

[urlp] http://www.osspa.cnipa.it/,.

[Zag00] R. Zagami. *Firma digitale e sicurezza giuridica.* CEDAM, 2000.