UNIVERSITÀ DEGLI STUDI DI PADOVA

Corso di Laurea Triennale in Ingegneria Elettronica

Tesi di Laurea

Applicazione della firma digitale ai documenti clinici

Relatore: prof. Alfredo Ruggeri

Correlatore: dott. Claudio Saccavini

Laureanda: Walnea Ceolin

Anno Accademico 2009/2010

A papà lassù,
a mamma quaggiù

"..., I know the road looks lonely,
but that's just Satan's game..."

Intervention - Madonna

Indice

1. PREMESSA DI CONTESTO

Il presente documento si propone di chiudere una prima fase di analisi di fattibilità dell'avvio di un sistema di conservazione della documentazione clinica ed amministrativa prodotta nelle Aziende Sanitarie appartenenti all'Area Vasta Veneziana.

Ritenendo che il processo di conservazione rappresenti solo uno dei passaggi fondamentali della gestione documentale digitale a pieno valore legale, si reputa indispensabile impostare l'avvio del rivoluzionario cambiamento verso l'informatizzazione in primo luogo attraverso la conoscenza e poi con l'utilizzo degli strumenti adatti.

Onde capire dove porre maggiormente l'attenzione, si è creduto importante eseguire una fotografia dello scenario odierno per la produzione di documenti in ogni singola Azienda Sanitaria. La consapevolezza dello *status quo ante* appare indispensabile ai fini di una responsabile analisi della fattibilità del cambiamento. La normativa vigente è sempre più orientata verso l'imposizione di una produzione ed una totale gestione dei documenti informatici, la necessità di adeguate ottimizzazione e riorganizzazione di processi e risorse vengono strenuamente avvertite dai decisori e dai diretti operatori, ma spesso la realtà quotidiana di alcuni settori applicativi rischia di cozzare con certi approcci semplicistici. Ma nel contempo il voler procrastinare eccessivamente il decollo di organici progetti di gestione documentale rischia di provocare distorti utilizzi della tecnologia e mostruosità fisiologiche, come verrà più volte sottolineato nel corso del presente documento.

La compilazione di un apposito questionario da parte delle Aziende Sanitarie dell'Area Vasta Veneziana e gli incontri presso le medesime da parte di alcune professionalità di Arsenàl.it (tecnologiche, organizzative e legali) con i Sistemi Informativi, le Direzioni Sanitarie e gli Affari Generali e Legali hanno permesso di raccogliere alcuni elementi importanti riguardanti dati, procedure, quesiti, desiderata ed osservazioni, volti a raffigurare il quadro odierno ed i bisogni di approfondimento. A questo riguardo si richiama, appunto, qui l'attenzione sugli allegati: Allegato A, dove viene proposta l'elaborazione dei dati raccolti attraverso il questionario proposto alle ULSS dell'area vasta veneziana.

2. LA DEMATERIALIZZAZIONE

2.1. INTRODUZIONE

Negli ultimi tempi il tema della dematerializzazione sta assumendo particolare rilevanza e attualità. Grazie anche all'impulso impresso dalla nostra politica per la modernizzazione della Pubblica Amministrazione attraverso nuove applicazioni tecnologiche, un quadro normativo coerente che cerca di tenersi al passo con le esigenze, un'organizzazione dedicata e una cultura su questi temi ormai diffusa, si è in grado di realizzare quei tanto desiderati benefici, in termini di risparmio e di efficacia, che la traslazione del documento dal supporto analogico a quello digitale ha da molto tempo prospettato. Con l'emanazione del Codice dell'Amministrazione Digitale viene data attuazione ai meccanismi rivolti a realizzare con concretezza l'assai bramata 'scomparsa della carta'.

Un disegno che impegna a una trasformazione profonda del modo di agire di ogni struttura, sia essa pubblica o privata, con pesante coinvolgimento delle proprie risorse professionali, ma anche con una gradita valorizzazione delle stesse.

Il concetto, ormai sedimentato, di documento informatico viene così tradotto dal Legislatore: "rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti", permettendo in tal modo di agire sui temi della gestione digitale dei flussi documentali e sulle condizioni tecnico-giuridiche e agevolando il passaggio dall'analogico al digitale.

Con la crescita della normativa di questi ultimi anni in materia, in parallelo alla tecnologia sviluppata, il governo dell'intero ciclo di vita del documento informatico deve fondarsi su tutti gli strumenti ritenuti necessari da ogni ambito (già facenti parte dello scenario analogico), ma deve nel contempo tener ben conto delle molte ricadute sugli aspetti organizzativi legali prodotti dal loro utilizzo.

La gestione con metodo informatico dei flussi documentali all'interno e all'esterno delle Strutture diviene quindi un momento fondamentale nei processi di cambiamento sia della Pubblica Amministrazione che del mondo privato. I vantaggi e le economie all'interno delle Strutture, che si stanno già tangibilmente percependo, saranno poi affiancate anche dal valore strategico che assumerà questa innovazione, quando i cittadini si sentiranno direttamente coinvolti e ne sentiranno i diretti effetti.

Al fine di permettere una massiva e omogenea gestione del documento informatico, è importante aver ben chiaro che non poche problematicità dovranno essere affrontate, così come qualsiasi cambiamento epocale ha dovuto sostenere. A livello trasversale, senza nemmeno prendere in considerazione gli specifici ambiti, già possono essere individuati comuni criticità, legate a volte alla difficoltà interpretativa della normativa vigente, alla scarsa diffusione di coscienza dei workflow dei documenti e delle loro caratteristiche giuridico-probatorie (valore e apposizione della sottoscrizione; significato ed uso di originali, copie e copie conformi; ecc. ...), alla scarsa fiducia nello strumento informatico che sembra non umanamente controllabile, alla difficoltà di consegna/visualizzazione/fruibilità del documento informatico.

Con il termine "dematerializzazione" è stata sin da subito identificata la *tendenza alla sostituzione della documentazione, solitamente analogica, in documento informatico*. Un termine ormai entrato nel lessico della gestione documentale e nella normativa, che gli ha conferito pieno valore legale. La dematerializzazione della documentazione è tema che (per le firme elettroniche, la conservazione sostitutiva, l'archiviazione ottica, il tempo informatico, ...) ha interessato prima la riforma della vita degli enti pubblici e privati e ora anche quella dei singoli cittadini. L'argomento è quindi divenuto di grande attualità ed ha coinvolto numerosi operatori e studiosi del settore, dando vita proprio alla colonna odierna della dematerializzazione, il D.lgs. 7 marzo 2005, n. 82 "Codice dell'Amministrazione digitale".
Al di là della mera creazione del documento informatico, il governo dei processi di gestione completa del documento è un fattore fondamentale per garantire ora e nel tempo l'integrità e la reperibilità del documento stesso. La dematerializzazione non può venire ricondotta alla mera realizzazione di processi di digitalizzazione della documentazione. Ciò invero è a volte accaduto inizialmente, con nefaste conseguenze, anche di totale abbandono delle scelte intraprese verso l'informatizzazione, per impreparazione a governare il grande cambiamento. La sfera dell'analisi, della riorganizzazione dei processi, della trasparenza e della conseguente assunzione di responsabilità da parte di ogni soggetto coinvolto, dell'utilizzo ormai quasi totale degli strumenti tecnologici nella comunicazione diventa il fulcro fondamentale per ottenere risultati in questo ambito.
Quindi la dematerializzazione viene a porsi oggi come il *processo qualificante di efficienza e trasparenza*, portando nel contempo sì a risparmi diretti in termini economici, sociali ed umani, ma anche e soprattutto di efficacia nel perseguimento degli scopi propri di ogni settore specifico.

A questo proposito, uno degli ambiti più studiati per l'individuazione e la quantificazione del 'costo sociale' è stata da subito la Sanità, ove il semplice ritiro di un referto di analisi è stato sottoposto ad una approfondita analisi, non solo dal lato della Struttura produttrice del documento, ma anche dall'ottica del cittadino, tenendo conto di numerosi ed eterogenei monetizzabili: età, occupazione, mezzo di trasporto, chilometraggio da casa alla Struttura Sanitaria, tempo di percorrenza per il tragitto, ecc..
Ancora una volta quindi si è cercato di dimostrare in tutti i modi che si può contare su soluzioni tecnologiche ormai più che adeguate a rispondere alle richieste dei vari settori e all'abbandono dell'analogico in favore del digitale.
Nel contempo, l'emanato normativo italiano può essere ritenuto come uno dei più avanzati a livello europeo ed internazionale tutto. Senza, peraltro, dimenticare che le norme in tema di dematerializzazione non possono vivere avulse dal contesto; si devono trovare pertanto in una posizione di trasversalità rispetto alle singole sfere di competenza (sanità, giustizia, fisco, lavoro, contrattualistica, ecc. …), con le loro peculiarità normative e le diverse esigenze utilizzeranno le regole sulla dematerializzazione calate nello specifico contesto quotidiano.

2.2. IL SIGNIFICATO DI DEMATERIALIZZAZIONE

Come già più sopra accennato, generalmente con il termine dematerializzazione viene intesa la "*tendenza alla sostituzione della documentazione amministrativa solitamente cartacea in favore del documento informatico"* (Libro Bianco del Gruppo di Lavoro interministeriale per la dematerializzazione tramite supporto digitale). Da questa generica definizione si evince pertanto che la dematerializzazione va intesa sotto due aspetti, anche correlati fra loro, ma con problematiche e soluzioni pratiche differenti:

- in primo luogo è gestione documentale totalmente informatica, con lo scopo di limitare la produzione di documenti analogici;
- è pure l'iter di trasformazione della documentazione analogica esistente in altra in formato digitale, eventualmente scartando quella ritenuta non necessaria a fini storici-culturali-legali.

Ma anche gli obiettivi sono due e assai differenti: da una parte si tende ad eliminare i documenti analogici attualmente rinvenibili negli archivi, trasformandoli in informatici e cercando di distruggere i primi attraverso lo 'scarto', se non soggetti a stringente tutela per il loro interesse storico-culturale; dall'altra si imboccano azioni per evitare o limitare notevolmente la creazione sin dall'inizio di nuovi documenti analogici.

Le problematiche e le soluzioni previste nei due scenari sono molto differenti.

2.3. TRASFORMAZIONE DELL'ANALOGICO ESISTENTE IN DIGITALE

Sin dall'inizio di questo documento si è tentato di far comprendere che uno dei precipui scopi della dematerializzazione/gestione documentale è di limitare la produzione di nuova documentazione su supporto analogico, ma anche quello di eliminare quella già esistente, nei casi in cui non risulti di interesse storico e quindi sottoposta alla normativa in materia dei Beni Culturali.
La trasformazione dell'analogico esistente in digitale, e la conseguente eliminazione del primo, esigono l'individuazione e la predisposizione di processi altamente qualificati: quando invero il documento nasce su supporto analogico e si vuole giungere alla sua totale dematerializzazione, se ne deve prevedere la scansione e l'acquisizione in formato digitale, affinché esso possa entrare nel ciclo di gestione documentale.
La gestione e la trasformazione in digitale della documentazione analogica, oggi esistente negli archivi, rappresentano solo una parte delle problematiche connesse alla dematerializzazione, e sono fonte di comprensibili timori per i problemi di natura giuridica che creano. Invero scarsa è la propensione manifestata dal Ministero degli Archivi e dei Beni Culturali verso la conversione da analogico ad informatico con il conseguente scarto della documentazione clinico-sanitaria, se il documento da sottoporre al procedimento ha in sé un forte valore giuridico e legale.

Nulla da eccepire riguardo alla perplessità degli addetti ai lavori archivistici in merito alla dematerializzazione dei documenti clinico-sanitari, con l'aggiunta della distruzione dell'analogico originale: i valori giuridico, legale e medico-legale di questa particolarissima documentazione fanno sempre più propendere per una scarsa fiducia nell'attività di trasformazione dalla carta al digitale, effettuata senza regole tecnologiche ed opportuno dominio sulle stesse e sulle metodologie operative. Qualora poi ci fosse la necessità di rinvenire l'originale analogico, per effettuare i necessari controlli di corrispondenza fra documento sostituito e digitale sostituente, si scoprirebbe che il primo è stato distrutto attraverso lo scarto.

Se alla luce dei dubbi procedurali, tecnologici e giuridici si decidesse di utilizzare il processo di trasformazione da analogico in digitale solo a fini di raccolta e reperimento delle informazioni pregresse, che senso avrebbe trasformare il vetusto analogico in moderno digitale, senza riuscire a dare al secondo dignità legale? E ancor peggio, senza poter nel contempo eliminare definitivamente l'analogico, disinteressandosene delle sorti perché più interessati al digitale, peraltro privo di un degno valore legale?

Per l'effettivo limitato guadagno (economico, organizzativo, funzionale, legale, …) apportato da questa modifica di supporto, si può qui affermare definitivamente che la dematerializzazione del pregresso analogico ha assai poco senso di essere sostenuta. Ciò soprattutto in ambito clinico-sanitario, ove la maggior parte dei documenti prodotti assumono da subito pregnanti valori giuridico e medico-legale. Cercar di sostituire i documenti cartacei con quelli informatici attraverso la loro scannerizzazione, per una mera più veloce consultazione delle informazioni in essi contenute, senza poter anche essere garantiti in ogni aspetto dalla totale legalità della metamorfosi, non ha senso alcuno.

Quindi la tendenza dei cultori della materia è quella di sconsigliare l'avvio di progetti di dematerializzazione pura che, in balia della speranza di modernizzare i processi della Struttura, potrebbero portare a trattamenti ibridi e sovrapposti, confusionari, poco legali e nel contempo altamente dispendiosi.

2.4. STRUMENTI DELLA DEMATERIALIZZAZIONE

Come precedentemente qui accennato, la nascita dei sistemi di gestione documentale informatizzata all'interno delle Strutture Sanitarie, sia private che pubbliche, porta inesorabilmente con sé parecchi dubbi e problemi di ordine giuridico, tecnologico, funzionale, archivistico e medico-legale, anche per ciò che concerne gli strumenti da implementare e calare nella concreta realtà operativa. Tutto ciò spinge ad una responsabile analisi delle criticità e comporta che vi debba sempre essere una rivisitazione dell'intera Struttura coinvolta, nel modo più omogeneo possibile, evitando gli interventi delimitati a pochi passaggi, oppure a modernizzazioni solo di piccole nicchie. Il concentrarsi su una preliminare analisi dello scenario che si vuole andare a modificare è doveroso, al fine di individuare tutti i soggetti interessati, le architetture tecnologiche e funzionali, le responsabilità in capo ad ognuno. La definizione puntuale dei modelli di gestione dei workflow documentali nell'intervallo che va dalla creazione alla conservazione e

post-conservazione del documento è indispensabile per poi non dover affrontare sgradite sorprese in corso d'opera.

Di seguito vengono individuati e, seppur superficialmente, analizzati i principali strumenti che la pratica e la normativa reputano indispensabili per avviare il processo di dematerializzazione: alcuni di essi sono comuni sia al mondo pubblico sia a quello privato, altri invece sono propri della Pubblica Amministrazione. Tali strumenti possono essere così individuati:

- il documento informatico
- le firme elettroniche (firma elettronica, firma elettronica qualificata, firma digitale)
- la classificazione e la fascicolazione
- la posta elettronica certificata
- l'archiviazione e la conservazione
- la protocollazione

L'introduzione normativa del d*ocumento informatico* è stata la prima pietra con cui si è dato il via alla gestione documentale digitale e alla dematerializzazione. Ma la gestione automatizzata del flusso documentale non si può fermare alla creazione del documento; si devono fare i conti con la gestione completa dei flussi, attraverso un'infrastruttura applicativa integrata con il protocollo, con i sistemi di pianificazione e controllo e di workflow per la gestione dell'iter procedimentale.

Con la diffusione dei sistemi per il *protocollo informatico* - obbligatorio nella Pubblica Amministrazione - e con la semplificazione e la razionalizzazione dei modelli organizzativi, la protocollazione ha visto irrobustire il suo ruolo.

Anche la *classificazione* è diventata un elemento indispensabile in un sistema documentario digitale. Infatti, essendo essa basata sull'organizzazione funzionale dei documenti, serve a consentire la corretta ed efficiente formazione dei fascicoli, l'integrazione con i piani di conservazione e con la gestione dei processi, oltre al fondamentale sia agevole che veloce recupero dei documenti, sfruttando le relazioni funzionali costituitesi nel corso dell'attività.

Nel contesto della trasformazione, anche gli strumenti archivistici sono andati modificandosi, peraltro senza subire rivoluzioni per ciò che concerne il loro funzionamento e le finalità.

Come in ogni modernizzazione, un periodo di governo ibrido deve essere inevitabilmente vissuto e alcuni dei campi di cambiamento possono risultare piuttosto nodali e nel contempo critici. Per esempio, la *firma digitale* (uno dei primi passaggi della gestione informatica di un documento) e la *conservazione ottica* (uno degli ultimi passi del processo) costituiscono i punti più delicati, poiché operativamente rappresentano una forte trasformazione che deve mantenere le sue potenzialità tecniche e legali nel tempo. Basti pensare che per una cartella clinica di ricovero, e di tutto ciò che essa contiene (come per esempio i referti firmati di Diagnostica per Immagini, Chimica Clinica, Microbiologia, Anatomia Patologica, …), vige l'obbligo di conservazione a tempo indeterminato.

Come è stato sopra accennato, è errato affrontare la dematerializzazione a settori di attività e si può affermare che è anche altrettanto sbagliato inserire nella fase di transizione solo alcuni degli strumenti a disposizione. Gli strumenti per una completa gestione documentale ci sono, da un punto di vista tecnologico; vanno quindi propriamente introdotti negli ambienti di interesse e customizzati a seconda delle specifiche esigenze.

2.5. DOCUMENTO INFORMATICO

E' corretto ricordare che tutte le informazioni che oggi gli umani si scambiano sono contenute in documenti analogici (con le caratteristiche proprie di fogli cartacei, pellicole, ecc.), totalmente human readable, ma poco riutilizzabili, copiabili, integrabili, lentamente ricercabili. Nella pratica elettronica, invece, molte delle informazioni esistenti non sono contenute in documenti veri e propri, ma possono essere dei meri messaggi o comandi informatici (come per esempio un messaggio HL7) che, collezionati ad hoc, potranno poi anche andare a comporre il contenuto di un documento.
Quando in questo lavoro si parla di gestione documentale ci si riferisce al documento vero e proprio, quale contenitore materiale delle informazioni precedentemente prodotte: un referto, una lettera di dimissioni, una fattura, un mandato di pagamento, …. E' per questo motivo che si ritiene utile prima comprendere il vero significato giuridico del 'documento' e poi calarlo pian piano nel mondo digitale.
Il codice civile individua tre tipi di documento esistenti:

- la scrittura privata
- l'atto pubblico
- la riproduzione meccanica

L'art.2702 del codice civile asserisce che "la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta". Il codice civile si sofferma, in modo abbastanza superficiale, ad individuare gli elementi essenziali per l'esistenza giuridica della *scrittura privata*: il documento deve essere composto da una dichiarazione scritta, proveniente dal soggetto interessato e sottoscritta da quest'ultimo. L'*atto pubblico*, previsto dal codice civile all'art.2699 in modo più puntuale, è invece "il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato."

Il codice civile nulla manifesta in tema di modalità di redazione di questi documenti, né si sofferma sui supporti o sui mezzi di scrittura, sulla firma e sulla conservazione dei documenti stessi. Essi possono quindi avere qualsiasi forma tecnologica, purché idonea a raggiungere lo scopo desiderato.

In tutti gli ambiti, e anche in quello clinico-sanitario, vi sono poi dei documenti che possono rientrare in quella categoria per la quale non è imposta per la sua esistenza giuridica una particolare ed indispensabile assunzione di responsabilità professionale del redigente, considerato che per essi non è richiesta forma predeterminata (certamente non scritta ad substantiam ex art.1350, n.13, c.c.) né obbligo di sottoscrizione: questi documenti sono quelli derivanti dalla definizione di cui all'art.2712 c.c., modificato dall'art.23 del D.lgs n.82/2005, riguardante la *riproduzione meccanica.* Essa viene così definita dal codice: "Le riproduzioni fotografiche o cinematografiche, le registrazioni fotografiche 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".

A partire dal 1997 le nostre norme nazionali hanno provveduto a riconoscere e ribadire il valore giuridico del documento informatico, equiparandolo nei suoi valori al documento cartaceo e definendolo come "la rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti" (art.1, co.1, lett. p del D.lgs n.82/05). Inoltre il Codice dell'amministrazione digitale, modificato dal D.lgs n.159/06, all'art.20 asserisce che "1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice. 1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta é liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2. 2. 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".

E' evidente quindi che il Legislatore ha voluto così ribadire la vasta portata giuridica e probatoria del documento informatico e della sua introduzione nei flussi documentali moderni.

2.6. SOTTOSCRIZIONE

Molti dei documenti trattati già oggi su supporto analogico, siano essi clinico-sanitari o amministrativi, necessitano di una redazione in forma scritta e buona parte necessita della sottoscrizione affinché essi nascano acquisendo valori giuridici, medico-legale e probatorio.

Più sopra è stato citato il significato di documento informatico, il quale non deve prescindere dalla più generale qualificazione degli atti/documenti che il nostro codice civile prevede: l'*atto pubblico* e la *scrittura privata* a cui va aggiunta la *rappresentazione meccanica*. Ma non bisogna nemmeno dimenticare che uno degli elementi essenziali, e caratterizzanti, del tipo di documento che si vuole andare a creare e

trattare è la sua sottoscrizione: non sempre essa è necessaria per infondere valore giuridico sin dalla nascita al documento, ma, se va apposta, deve avere delle specifiche caratteristiche.
A fini esemplificativi, si porta l'esempio della documentazione clinico-sanitaria: referto, immagine, certificato, referto medico-legale, cartella clinica, lettera di dimissioni, ricetta, …. Cercando di inquadrare il referto, vanno rinvenuti significati diversi a seconda del soggetto che lo stende e del contesto in cui esso viene redatto, per fargli ottenere anche valenze legali e probatorie differenti. Il *referto* diagnostico è l'atto, obbligatoriamente redatto in forma scritta e sottoscritto, col quale il medico specialista dichiara conformi a verità i risultati delle indagini o degli esami ottenuti, unitamente all'interpretazione clinica dei risultati stessi, in relazione al quadro clinico e all'anamnesi del paziente. E' il documento che entra a pieno titolo nella categoria della scrittura privata. Del contenuto del referto vi deve essere un'assunzione di responsabilità da parte di colui che lo ha redatto; è proprio la sottoscrizione che attribuisce la paternità dell'atto e permette, anche in un momento successivo, di risalire all'autore di questo. Infatti, proprio in base all'art. 2702 del Codice Civile, il referto per avere dignità giuridica e per ottenere valore legale e probatorio deve essere sottoscritto dal medico refertante.
Come già accennato, secondo il diritto gli atti pubblici devono invece possedere requisiti ben individuati e devono essere redatti da un pubblico ufficiale. Per il referto diagnostico, le norme vigenti non prevedono alcuno dei rigidi requisiti dell'atto pubblico codificato. Mentre tali elementi possono essere rinvenuti per il certificato, il referto medico-legale, la cartella clinica,... Il c*ertificato* o il *referto medico-legale* sono documenti a cui il medico è obbligato (per esempio in base anche all'art.22 del Codice di deontologia medica 1998) e nei quali deve limitarsi ad attestare i dati obiettivi di competenza tecnica che abbia direttamente constatato in totale aderenza alla realtà.

Il *risultato* (immagine radiologica, valore glicemico, filmato di emodinamica) invece, pur dovendo essere rappresentato in un documento anch'esso, è il puro esito degli esami diagnostici eseguiti mediante strumentazioni cliniche in un'indagine (Laboratorio, Radiologia, …); è un prodotto privo di interpretazione o valutazione clinica da parte dello specialista, ovvero una lettura pura e semplice di un dato analitico. Ecco perché si ritiene non debba essere corredato da sottoscrizione, mancando l'obbligo di assunzione di paternità e responsabilità umana da un punto di vista sostanziale. Il risultato può quindi avere qualsiasi forma tecnologica, purché idonea a raggiungere lo scopo desiderato. Si è certi di poter affermare che il risultato diagnostico sia un tipico esempio di rappresentazione meccanica, come lo possono essere i preparati istologici e citologici. La stessa Circolare Ministero della Sanità n.61 del 19 dicembre 1986, N.900.2/ AG.464/260, concernente il "Periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura", asserisce che le radiografie non rivestono 'il carattere di atti ufficiali', ma sono i dati su cui si deve basare la refertazione diagnostica del medico specialista. Mancando l'iconografia, come gli altri risultati, di un intrinseco atto medico e dell'indispensabile assunzione di responsabilità professionale per esso, gli elementi essenziali che ne possono definire la giuridica esistenza sono quelli derivanti dalla definizione di cui all'art.2712 Cod. Civ. modificato dall'art.23 del D.Lgs. 82/2005 (riproduzione meccanica nel genere e informatica nella specie,

se di documento informatico si tratta), considerato che per essa non è richiesta forma predeterminata (certamente non scritta ad substantiam ex art.1350, n.13, Cod. Civ.) né obbligo di sottoscrizione.

Risulta evidente che già l'apparentemente vecchio codice civile basava le differenze fra i documenti sulla necessità che essi venissero sottoscritti oppure no. Quindi, nel passaggio dal mondo analogico a quello digitale nulla cambia riguardo ai principi fondamentali su cui si basano la nascita e il valore giuridico di un documento. La sottoscrizione rimane l'elemento fondamentale. La trasformazione da documento analogico in documento digitale porta a mutare la sottoscrizione autografa in una delle firme elettroniche che verranno qui di seguito analizzate.

2.6.1. *La famiglia delle firme elettroniche*

Pian piano verrà qui chiarito come la sottoscrizione informatica si differenzia dalla sottoscrizione autografa, non solo per il supporto sul quale viene apposta. Comunque l'utilizzo del termine 'firma' non deve generare nell'operatore un timore maggiore di quello che esso gestisce, invece, in modo del tutto tranquillo durante la propria giornata lavorativa attraverso l'utilizzo degli altri strumenti tecnologici.
A questo punto vanno richiamate le tipologie di sottoscrizione informatica e le loro definizioni di legge:

- **La "firma elettronica"** ***cosiddetta leggera*** (D.lgs. n.82/05, art. 1, comma 1, lett. q, modificato dal D.lgs 4 aprile 2006 n.159 in G.U. n.99 del 29 aprile 2006": "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica"
- **La "firma elettronica qualificata"** ***cosiddetta forte*** (D.lgs. n.82/05, art. 1, comma 1, lett. r, modificato dal D.lgs. 4 aprile 2006 n.159 in G.U. n. 99 del 29 aprile 2006): "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".
- Nel genere firma elettronica qualificata è da inquadrare la "firma digitale" (D.lgs n.82/05, art.1, comma 1, lett. s): È "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

Oltre alle stringate definizioni della norma, che poi verranno più avanti approfondite da un punto di vista tecnologico, ci si deve soffermare su alcune valutazioni di ordine giuridico. A seconda della tipologia di firma, anche il documento a cui essa viene apposta acquisisce un valore legale e probatorio diverso:

- il documento informatico sottoscritto con *firma elettronica* è liberamente valutabile in giudizio, Tenuto conto. Sarà affidata alla discrezionalità motivata del giudice stabilire se il documento soddisfi il requisito della forma scritta e quindi il valore probatorio, tenendo conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21, comma 1, D.lgs. n.82/05);
- il documento informatico sottoscritto con *firma elettronica qualificata* ha *l'efficacia della scrittura privata* (in base ad una presunzione semplice, consente di attribuire la paternità delle dichiarazioni contenute nel documento, al suo sottoscrittore con firma digitale o elettronica qualificata). Previsione dell'art.2702 del Codice Civile (art.21, comma 2 D.lgs n.82/05), con piena risposta al requisito della *forma scritta* (forma scritta "ad substantiam" ex art.1350 cod. civ. numeri da 1 a 12, e art.20, comma 3 D.lgs. n.82/05).

L'innovazione dell'art.21, comma 2 è evidente quando equipara il documento informatico digitalmente sottoscritto al documento analogico cui sia apposta una sottoscrizione autografa, se il documento deve essere portato ed utilizzato in giudizio.
Sia per il documento cartaceo firmato autografamente sia per il documento informatico digitalmente sottoscritto, il valore probatorio ha natura presuntiva (ovvero si presume che sia stato redatto e firmato da colui che appare il sottoscrittore) potrà essere neutralizzato esclusivamente dalla persona contro la quale esso verrà prodotto in giudizio e ne disconoscerà la firma digitale. Verrà negata in questo modo la paternità delle dichiarazioni in esso contenute e rifiutate le conseguenti responsabilità.

A questo proposito, trattandosi di sottoscrizione generata dall'utilizzo di dispositivi basati su tecnologie semplici ma particolari, il titolare della firma, potrà provare in sede di disconoscimento della firma stessa, che tale utilizzo di dispositivi e tecnologie non sia a lui attribuibile, ad esempio a causa di abuso compiuto da un terzo che abbia sottratto il dispositivo di firma.
Il disconoscimento in sede di giudizio della firma digitale apposta su documento informatico, provocherà l'inevitabile sua assoluta inutilizzabilità probatoria nel processo: il giudice non potrà pertanto decidere alcunché sulla base di esso se, ex art. 216, 2° comma, c.p.c., la parte che intende giovarsene (contro il presunto sottoscrittore) non ne avrà richiesta la verifica o questa non ottenga esito positivo.

2.6.1.1. Le firme elettroniche da un punto di vista tecnologico

Al giorno d'oggi, la maggior parte dei documenti vanno sottoscritti e firmati, affinché abbiano valore legale. Così succedeva per la firma autografa e così continua a succedere con la firma digitale, purché essa sia apposta secondo le norme vigenti.
Come prima cosa possiamo affermare che a garanzia di quanto appena detto c'è la legge del 15 marzo 1997 n.59, art.15, comma 2:

(…) 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. Gli schemi dei regolamenti sono trasmessi alla Camera dei Deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni. (…)

Viene sancita quindi la piena rilevanza e validità giuridica anche se effettuata in forma elettronica, e ciò va ad integrare quanto precedentemente disciplinato dal codice civile del 1942. La norma coinvolge indifferentemente sia i soggetti privati sia la pubblica amministrazione.

Appurato questo, prima di cominciare con i dati tecnici, esaminiamo una comparazione tra le firme attualmente esistenti, analogica (autografa) e digitale.
Innanzitutto, nessuna norma impone che il supporto materiale del documento sia esclusivamente quello cartaceo, perciò ne deriva che quanto basta a soddisfare il concetto di scritto è che si lasci una traccia duratura e leggibile sia al momento della scrittura, sia a distanza di tempo, a prescindere dal tipo di alfabeto e di supporto usato: ne consegue che l'immaterialità del documento informatico non costituisce un problema e, come si è già visto, è sufficiente garantire la provenienza e l'immutabilità del documento, ovvero che i contenuti dello stesso non vengano modificati dopo la loro formazione: sucidamente entrambe le esigenze nel documento analogico sono garantite dalla materialità del supporto (la carta) e dalla sottoscrizione dell'atto da parte di colui che ne assume la paternità.
Queste caratteristiche, che sono proprie dei supporti analogici, mancano effettivamente nel supporto informatico, poiché le registrazioni effettuate sono di norma non indelebili e non consentono la riconoscibilità di eventuali alterazioni; inoltre, il documento informatico, pur essendo ormai riconosciuto come documento scritto, non può evidentemente essere sottoscritto in modo tradizionale mediante l'apposizione autografa del nome e del cognome dell'autore. Però, la soluzione a tali ostacoli, come vedremo nei paragrafi successivi, è data dalla firma digitale.
Per come è strutturata la firma digitale, essa è associata stabilmente al documento informatico e lo arricchisce di informazioni che attestano con certezza l'integrità, l'autenticità e la non ripudiabilità dello stesso.

Fondamentalmente possiamo analizzare:

Creazione: mentre la firma analogica viene apposta in modo manuale, nel caso di quella digitale essa viene apposta mediante opportuno algoritmo di creazione, che fa già presagire una sottoscrizione più sicura; inoltre, mentre lo strumento analogico - la penna - può essere impugnato da chiunque, nel

digitale il dispositivo di firma è sicuro e il firmatario ha l'uso e il controllo esclusivi su di esso.

Apposizione: la firma autografa diventa parte integrante del documento, mentre con la modalità di firma digitale si tende a pensare alla firma come un allegato, dove il documento firmato è costituito dalla coppia documento e firma. C'è da precisare però, che a seconda del tipo di firma digitale usato, questa visione della firma allegata può variare, fino al caso in cui la firma viene contenuta nel documento stesso, ma questo sarà oggetto di discussione specifica fra qualche paragrafo.

Autenticità & Integrità: otteniamo indiscutibilmente la garanzia dell'identità di chi firma, associata senza dubbi al sottoscrivente, così come da controlli sui documenti anagrafici precedentemente avvenuti, in sede di assegnazione delle chiavi di firma; da notare che esiste una differenza sostanziale tra l'autenticazione applicabile ad una firma autografa, che avviene attraverso il confronto con altra firma, e la verifica della firma digitale che avviene presso il certificatore mediante chiave pubblica. I due procedimenti non hanno lo stesso valore, infatti, nel secondo caso è improprio parlare di autenticazione in quanto manca un pubblico ufficiale che attesti che quella firma è stata apposta in sua presenza. Ma l'autenticazione, comunque, viene fatta a priori al momento della consegna della smart card anziché contestualmente al momento in cui si firma.

Provenienza: il risultato della firma attraverso l'uso delle chiavi è quello che la connessione tra firmatario e documento firmato sia univoca, amplificando ancora il regime di sicurezza;

Verifica: quando ci si ritrova a dover verificare l'autenticità di una firma autografa, si può procedere solo al confronto con una firma autenticata, ma rimane un metodo insicuro, poiché, nel peggiore dei casi, nemmeno una perizia calligrafica può assicurare con certezza che la firma in oggetto non sia una copia. Nel caso della firma digitale, tale verifica avviene solo attraverso un algoritmo di verifica, pubblicamente noto, e otteniamo un metodo sicuro.

Integrità: a differenza di quanto succede nel documento cartaceo, altamente modificabile, in quello digitale con firma digitale c'è la garanzia che il documento non sia stato manomesso né prima né dopo la sottoscrizione;

Documento copia: nel primo caso, qualsiasi copia venga stilata, rimane tale e quindi è facilmente distinguibile. Nel secondo caso, posso riprodurre dei file analoghi al primo firmato, che possono essere distinti nella forma, controllandone l'orario di creazione. Nella sostanza rimangono identici. Differente è il discorso se produco una rappresentazione del documento firmato digitalmente: esso rimarrà una rappresentazione e in quanto tale sarà banalmente distinguibile dall'originale da cui è stato prodotto.

Non ripudio: l'autore non può disconoscere il documento che risulti firmato con il suo nome e con i suoi strumenti. Rispetto la firma analogica, in questo caso la falsificazione diventa tremendamente più ardua.

Validità temporale: con il metodo tradizionale è garantita una illimitata validazione temporale, senza nessun vincolo o restrizione. Nel caso digitale, la sua validità temporale è legata alla stessa del certificato di autenticazione, e quindi essa è limitata, per ora, ad un periodo più breve, di 3 o 5 anni al massimo.

Automazione dei processi: se si volesse in un unico momento, firmare svariati documenti, nel modo classico ciò non risulta essere possibile. I mezzi in uso non ci permettono di fare ciò, dal lato meccanico (non esistono penne che firmano contemporaneamente su più fogli) né dal lato giuridico (la firma generata su più fogli mediante l'uso di carta carbone non ottiene il riconoscimento giuridico).

Valore legale: il documento elettronico sottoscritto digitalmente ha lo stesso valore legale di un documento cartaceo sottoscritto con firma autografa, secondo quanto già ribadito nella legge del 15 marzo 1997, art.15.

Certezza di arrivo a destinazione: La firma digitale consente anche, a chi ha firmato ed inviato i documenti in via telematica, di sapere con certezza quando i documenti stessi siano stati effettivamente ricevuti dal destinatario.

Continuiamo facendo alcune precisazioni e considerazioni: in primo luogo bisogna distinguere tra irripudiabilità tecnica e disconoscibilità giuridica. Dal punto di vista tecnico, infatti, la firma digitale non è suscettibile di critica, essendo una sorta di codice personale, la cui esclusività ed associazione all'utente viene garantita da un certificato, emesso da apposite società. Tradotta in termini giuridici, questa affermazione comporterebbe di considerare la firma digitale una sorta di prova assoluta, insuscettibile anche di un giudizio di falsità. E' invece importante mantenere uno spazio di critica, almeno a livello giuridico, ricorrendo ai principi generali dell'ordinamento ed adattando gli strumenti tradizionali di critica processuale (disconoscimento, istanza di verificazione e querela di falso) alla nuova realtà.
Quando, dunque, si vuole negare o disconoscere la propria sottoscrizione, si ricorre essenzialmente all'analisi grafologica, la quale individua il segno distintivo strettamente collegato alla persona sottoscrivente. Questo non è possibile nella firma digitale, essendo costituita da un insieme di lettere e cifre, il cui contenuto e la cui valenza risulta prefissata dalla legge. Il disconoscimento, pertanto, si configurerà in modo del tutto particolare nel documento informatico sottoscritto con firma digitale. Esso, infatti, potrà consistere nell'eccezione che la firma digitale sia stata applicata impiegando una chiave privata da parte di chi non ne era legittimo titolare, provocando così un'inversione dell'onere della prova: spetterà, infatti, alla persona che appare come sottoscrittore dimostrare la falsità della firma.

Concludendo, possiamo affermare che la firma digitale non porta a nessun tipo di svantaggio rispetto quella analogica, e se alcuni svantaggi sembrano essere presenti in prima battuta, con uno studio più approfondito della questione, risultano scomparire; emergono, invece, alcuni benefici dal suo uso.

A questo punto, è giunto il momento di cominciare a parlare dei vari tipi di firma attualmente esistenti:

- la firma elettronica
- la firma elettronica qualificata
- la firma digitale

2.6.2. *Firma elettronica quale sistema di autenticazione*

Richiamando la definizione del D.lgs. n.82/05, art. 1, comma 1, lett. q, modificato dal D.lgs 4 aprile 2006 n.159, secondo la quale la firma elettronica è "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica", si evidenzia che essa è considerata un sistema di autenticazione. Si cerca qui di seguito quindi di dare una visione del significato di sistema di autenticazione, preso bene in considerazione anche dal D.lgs n.196/03 e dal suo Allegato B per il trattamento dei dati personali. Ciò a dimostrazione che non vi sono, in questa materia, norme da analizzare ed applicare a compartimenti stagni; l'oggetto principale è la documentazione clinico-sanitaria, che va sviscerata in tutti i suoi aspetti e per il trattamento della quale debbono essere applicate norme apparentemente del tutto eterogenee fra loro nella materia. Quindi, anche se ci si trova qui nel capitolo dedicato alla sottoscrizione ed alle firme elettroniche apparentemente non correlate in modo alcuno alla data protection, è invece evidente che non vi è solo un legame ma una vera e propria compenetrazione dei concetti di base.

Autenticazione informatica

Dall'art.34 lett.a, nel D.lgs n.196/03 viene prevista la misura dell'autenticazione informatica, comprendente i mezzi (programmi informatici o componenti hardware) incaricati di verificare e convalidare l'identità e le credenziali di un soggetto, garantendo il controllo su chi accede al sistema e vi si muove all'interno.

Adozione di procedure di gestione delle credenziali di autenticazione

Quanto sopra risulta possibile grazie all'*adozione di procedure di gestione delle credenziali di autenticazione*, ossia quelle previste dall'art.34 lett.b del D.lgs n.196/03, le quali consistono in "dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica".

Nell'odierna accezione del controllo degli accessi, le credenziali sono costituite da qualcosa che il soggetto interessato 'conosce' (un codice identificativo o una password), 'possiede' (una smart card o un token) oppure 'è' (una caratteristica biometrica).

Al punto 3 del Disciplinare Tecnico viene previsto espressamente che ad ogni incaricato siano "assegnate o associate individualmente una o più credenziali per l'autenticazione". I due termini 'assegnate' e 'associate' riguardano le due diverse tipologie di credenziali: invero, una password può essere assegnata, ma non può essere assegnato un tratto biometrico (poiché esso è patrimonio esclusivo del soggetto) per il quale deve essere richiamato solo il concetto di associazione (e non invece di assegnazione).

Ancora il Disciplinare Tecnico al punto 4 asserisce che "Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato".
Questo è importante che venga anche normativamente sottolineato, a dimostrazione di quanto sia importante che la creazione, la gestione e la custodia delle credenziali siano sentite anche dal Legislatore come passaggi strategici. Infatti, al punto 5 del Disciplinare Tecnico vengono indicate le caratteristiche che obbligatoriamente deve possedere una password, oltre alle regole di composizione e di utilizzo della medesima, affinché si possa effettivamente garantire un livello minimo di sicurezza del sistema: la parola-chiave dovrà essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; inoltre la password non deve contenere riferimenti facilmente riconducibili all'interessato, deve essere modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni sei mesi, che si abbassano a tre in caso di trattamento avente ad oggetto dati sensibili e giudiziari.

Utilizzo di un sistema di autorizzazione

In un momento successivo all'avvenuta identificazione, un sistema di autenticazione permetterà al soggetto incaricato, espressamente autorizzato e designato, di trattare le informazioni. Il sistema di autorizzazione è definito dall'art.4, co.3 del D.lgs n.196/03 come "l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente", così come previsto anche dall'art.34 del medesimo decreto.

Profilo di autorizzazione

L'individuazione dei trattamenti consentiti va a costituire il profilo di autorizzazione, previsto specificatamente per ogni singolo utente e definito dall'art.4, co.3, lett.o) come "l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti". Inoltre il punto 14 del Disciplinare Tecnico così prevede: "Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione". Ad ogni soggetto utilizzatore dei sistemi viene permesso il trattamento dei dati in modo scalare e modulare: per esempio, in merito alla visualizzazione, alla modifica, alla cancellazione; oppure alla conoscenza di tutti i dati, o invece solo di quelli personali e non di quelli sensibili, all'utilizzo di un isolato sistema informatico, o di tutto il sistema informativo della Struttura (inteso come l'insieme di più sistemi informatici), etc.
Del tutto correlata alla misura dei profili di autorizzazione è quella prevista dalla lett. d dell'art.34 del Codice, finalizzata alla periodica revisione delle autorizzazioni per il trattamento dei dati, nonché alla individuazione delle operazioni consentite agli addetti alla manutenzione ed agli addetti alla gestione degli strumenti hardware e software. La lista degli incaricati ed i relativi profili di autorizzazione - viene

precisato al punto 15 del Disciplinare - può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Firma elettronica

La firma elettronica, o firma elettronica "debole", è una qualunque connessione di dati utile per l'autenticazione informatica, avvenuta su un documento elettronico. Si tratta però di uno strumento che offre scarse garanzie, perché non rispetta i requisiti tecnici e organizzativi di sicurezza previsti per le firme elettroniche forti. Rappresenta una firma elettronica generica che può essere realizzata con ogni strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un discreto livello di autenticazione dei dati elettronici; dunque, PIN e password costituirebbero, secondo le linee guida, uno strumento per la realizzazione di una firma elettronica solo se, attraverso esse, è possibile validare i dati elettronici. Per realizzare anche la funzione (diversa) di identificazione in modo univoco del firmatario, è necessario utilizzare la firma elettronica avanzata (che analizzeremo nel paragrafo successivo). Il documento elettronicamente sottoscritto con tale firma elettronica sarà riconosciuto dall'ordinamento come forma scritta e la sua efficacia probatoria potrà essere liberamente valutata dal giudice. Quanto detto è validato dalla versione 1.1 delle Linee guida per l'utilizzo della firma digitale, elaborata dal CNIPA e pubblicata il 31 maggio 2004, e risulta, per ora, l'ultimo passo italiano rispetto la direttiva europea 199/93/CE.

2.6.3. *Firma elettronica qualificata e firma digitale*

Firma elettronica qualificata

1. Andiamo a soffermarci sul significato delle parole "firma digitale": dal D.lgs n.82/05, art.1, co.1, lett. r, modificato dal D.lgs n.159/06, si evince che la firma digitale è definita come «*il risultato della procedura informatica 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 di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*».
2. Ancora, il Codice dell'Amministrazione Digitale, Art.21 comma 2 recita: "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 sia data prova contraria". In sostanza il valore legale della firma digitale è equiparato a quello di una firma autografa su una scrittura privata.
3. Riassumendo, la firma elettronica qualificata è una firma elettronica avanzata che consente una

stretta connessione tra l'oggetto sottoscritto e la firma, e quindi i dati contenuti nel certificato del titolare. La firma elettronica qualificata viene creata attraverso un dispositivo sicuro per la generazione delle firme, ossia una smart card rilasciata da un certificatore e basata su di un certificato qualificato (firma elettronica "forte").

4. Un certificato qualificato è un certificato che possiede determinate caratteristiche sancite dalle norme vigenti.

5. Tale tipologia di firma elettronica, più sofisticata dal punto di vista tecnologico e telematico, consente di identificare in modo univoco il firmatario. Al documento, la cui firma è basata su un certificato qualificato e creata con dispositivo sicuro, è riconosciuta un'efficacia probatoria, in modo che il titolare, per disconoscere il documento dovrà attivare il complesso procedimento della querela di falso.

6. Sostanzialmente, la firma digitale è un tipo di firma qualificata, la quale utilizza particolari tecnologie crittografiche.

7. Nell'ambito del sistema di chiavi crittografiche asimmetriche, il documento può venire cifrato in modi diversi. In particolare, il mittente può cifrare il documento con la chiave pubblica del destinatario, facendo acquisire a quest'ultimo la certezza in ordine alla segretezza del documento, poiché egli è l'unico in grado di decifrarlo con la sua chiave privata; può poi cifrare il documento con la propria chiave privata e questa modalità conferisce al destinatario la garanzia in ordine alla provenienza del messaggio; infine il documento informatico potrà essere cifrato dal mittente con la propria chiave privata e con la chiave pubblica del destinatario e ciò conferirà certezza in ordine alla segretezza, all'integrità ed alla provenienza del medesimo.

8. Dal punto di vista probatorio, un documento sottoscritto con firma elettronica qualificata ha l'efficacia di scrittura privata prevista dall'art.2702 del codice civile (art. 21, co.2, D.lgs n.82/05) e risponde al requisito della forma scritta (art. 20, co.3, D.lgs n.82/05).

9. Volendo essere precisi, mettiamo in evidenza che la firma digitale non deve essere confusa, nel modo più assoluto, con la digitalizzazione della firma autografa, ovvero la rappresentazione digitale di un'immagine corrispondente alla firma autografa. La prima, per quanto appena detto, ha piena validità legale, ed è un modo alternativo alla firma autografa. Il secondo, invece, è solamente una rappresentazione di una firma, è un'immagine, perciò non ha nessun valore a livello giuridico e probatorio.

Firma digitale

Anche in questo paragrafo, come nel precedente, si fa riferimento al già citato D.lgs n.82/05, art. 1, co.1, lett.s, dove viene data la definizione di firma digitale. Possiamo fare la seguente distinzione all'interno

della firma digitale: "*leggera*" oppure "*pesante*" (o "*forte*", o "*qualificata*"), a seconda del grado di sicurezza che garantisce.

Per "*firma pesante"* ci si riferisce ad una firma elettronica che soddisfi i seguenti requisiti:

1. essere connessa in maniera unica al firmatario;
2. essere idonea ad identificare il firmatario;
3. essere creata con mezzi sui quali il firmatario possa conservare il proprio controllo esclusivo;
4. essere collegata ai vari dati cui essa si riferisce, in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

In base alla normativa italiana, che ha recepito le disposizioni in materia di firma elettronica emanate a livello europeo, solo adempiendo pienamente ai requisiti, si può sostenere che la firma digitale sia in grado di esplicare la medesima efficacia di quella autografa e possa rendere i documenti validi e rilevanti a tutti gli effetti di legge.

La "*firma leggera*", a differenza di quella *"pesante"*, non può essere equiparata alla firma autografa e non è idonea a rendere i documenti validi e rilevanti a tutti gli effetti di legge, in quanto non vi è la presenza di un ente certificatore esterno e qualificato. Essa può essere usata in ambiti ristretti, in cui due o più soggetti si accordano sul valore da dare a tale firma al fine di accettare specifici documenti, verificando che provengano dall'intestatario (ad esempio all'interno di società, banche o assicurazioni che offrano ai clienti dei sistemi di sottoscrizione elettronica in modo da riconoscere dei documenti o degli ordini).
La firma digitale, tanto quella "*leggera*" quanto quella "*pesante*", si basa su di un sistema cosiddetto a "chiavi asimmetriche" (o a "chiave pubblica" o a "doppia chiave"): in pratica due serie di caratteri alfanumerici, appositamente generati, di cui una conosciuta dal solo firmatario (chiave segreta), e l'altra conoscibile da chiunque (chiave pubblica). La chiave segreta è necessaria ad apporre la firma, la chiave pubblica a verificare che il documento provenga effettivamente dal titolare. La sicurezza di un simile sistema risiede nel fatto che ad ogni chiave pubblica corrisponde una sola chiave privata, e che, con la conoscenza della sola chiave pubblica, è quasi impossibile riuscire a risalire alla chiave privata.
Per garantire la corrispondenza tra "chiave pubblica" e "chiave privata", nonché la titolarità delle chiavi in capo al soggetto firmatario, si ricorre ad un Ente Certificatore (ad es. InfoCamere o Poste Italiane), un soggetto terzo il cui compito istituzionale è appunto quello di garantire la certezza della titolarità delle chiavi pubbliche (attraverso dei cosiddetti " certificati") e di rendere conoscibili a tutti le chiavi pubbliche (attraverso un elenco telematico). Anche per garantire che la firma apposta abbia i requisiti richiesti, la firma digitale "*forte*" deve passare sempre attraverso la validazione di un Ente Certificatore esterno, che operi secondo procedure rigorose e a loro volta "certificate"; tali enti sono presenti in un elenco pubblico, e devono rispondere a tutta una serie di certezze di carattere tecnico e materiale.

Si può affermare che la firma digitale è il risultato di una procedura informatica che dà per certe l'autenticità e l'integrità dei documenti formati con mezzi informatici; ovvero essa è un surrogato della sottoscrizione autografa apposta ad un documento analogico. Con l'elemento dell'autenticità si ha la presunzione che la firma applicata al documento informatico appartenga al firmatario; con il requisito dell'integrità si ha la sicurezza che il documento non sia stato manipolato dopo la sua sottoscrizione.

L'utente che volesse far uso della firma digitale deve necessariamente dotarsi di un "*Kit per Firma Digitale*"**,** sommariamente composto da:

- dispositivo sicuro di generazione delle firme (smart card);
- lettore di smart card;
- software di firma e verifica.

Installato il Kit sul proprio computer, attraverso il software di firma sarà possibile scegliere il certificato con il quale si intende firmare e, inoltre, si potrà selezionare il documento elettronico da sottoporre a firma digitale.
La scelta del certificato si rende necessaria in quanto ogni dispositivo può contenere più certificati rilasciati, al medesimo titolare, per scopi diversi (es. un certificato rilasciato al titolare in qualità di cittadino, un altro certificato rilasciato alla stessa persona nella sua qualità di legale rappresentante di un'azienda).
E' evidente come la firma di un documento informatico avvenga attraverso l'uso di un dispositivo (smart card) contenente le informazioni sul titolare del dispositivo stesso (certificato di sottoscrizione rilasciato dall'ente certificatore), e attraverso l'uso di un software appropriato che sia conforme a quanto indicato nell' art.35 del Codice dell'Amministrazione Digitale (C.A.D.) ed alle Regole Tecniche richiamate all'interno del C.A.D. stesso. Le smart card e il software fornito da diversi fornitori risultano conformi alla normativa vigente.
Al momento della firma del documento, il software chiederà l'inserimento del codice di protezione del dispositivo (PIN) e, se correttamente inserito, procederà con la verifica della firma e con la creazione del file firmato digitalmente.
Il file generato al termine del processo di firma sarà in definitiva una busta crittografica che conterrà vari elementi, variabili a seconda del tipo di firma, ma che fondamentalmente non discostano molto da questo gruppo: il documento originale (o il suo riferimento), le eventuali trasformazioni allo stesso, gli algoritmi di crittografia e firma, l'impronta firmata e il certificato digitale del firmatario.

Al momento attuale, secondo quanto dettato dalla "Guida alla firma digitale" emesso dal CNIPA nella versione v1.3 in data di aprile 2009, si prevede l'utilizzo di tre formati:

- Firma digitale in formato PKCS#7
- Firma digitale in formato PDF
- Firma digitale in formato XML

2.6.4. *Tipologia di firma*

2.6.4.1. Firma digitale in formato PKCS#7 (detta p7m)

Legislazione

Questo formato che risale a DPCM 8 febbraio 1999 rimane, senza ombra di dubbio il primo, che sia mai stato usato in Italia, e in quanto tale é quello che le Pubbliche Amministrazioni sono obbligate ad accettare. E' il formato più noto, in cui si firma attraverso l'uso della smart card.
In questo primo caso in esame, la firma digitale è un processo matematico secondo lo standard S/MIME (standard per la protezione dei messaggi di posta elettronica), che permette di criptare una rappresentazione univoca del documento (file) in esame, detta '*impronta*', e di inserirla nel file stesso trasformandolo in un nuovo tipo di file, con un'estensione propria: infatti il risultato del processo di firma di un file è un altro file, di formato diverso. Ad esempio, il file in formato Microsoft Word 'Documento.doc', al termine del processo di firma diventa il file 'Documento.doc.p7m'. L'estensione 'p7m' rappresenta la busta informatica (PKCS#7) e significa che il file non è più un documento Microsoft Word e quindi non può più essere aperto da questo stesso programma. In pratica, il documento viene sottoposto ad un processo di crittografia, solitamente asimmetrica ("a doppia chiave", con chiave pubblica e chiave privata, a 128 bit o più) e di tipo RSA. Per poterlo leggere è necessario l'uso di un nuovo programma, reperibile anche su internet, prodotto da varie software houses. Questo programma ha lo scopo di estrarre nuovamente il file originale e di confermare l'autenticità dell'autore del documento.

Modo d'uso

I passi principali del processo di firma si articolano nel seguente modo:

1. Creazione dell'impronta del documento: attraverso un algoritmo detto 'algoritmo di Hash' (Secure Hash Algoritm, SHA-1) è possibile estrarre un numero di lunghezza fissa (160 bit) detto "impronta" che ha la caratteristica di rappresentare univocamente il documento. Se viene cambiata una sola virgola al documento, anche l'impronta che lo rappresenta cambierà.

2. Firma dell'impronta: un altro algoritmo matematico permette di criptare l'impronta (che è un numero) definendo così un altro numero, chiamato "chiave privata". Questa operazione è molto semplice da effettuare, ma è a livello computazionale risulta molto difficile, soprattutto quando si tratta di effettuare l'operazione inversa, cioè ricavare la chiave privata. L'impronta così criptata è quindi sicura e non può essere alterata. La chiave privata viene creata sempre in coppia con un altro numero, chiamato "chiave pubblica". Quest'ultima permette di estrarre l'impronta criptata, ma non di criptarla.

3. Creazione del nuovo formato di file. Questa operazione può essere immaginata come la creazione di una sorta di busta all'interno della quale trovano posto:
    1. il file originale;
    2. l'impronta firmata;
    3. la chiave pubblica;
    4. il certificato dell'autore: rappresenta una vera e propria carta d'identità elettronica, rilasciato da un'autorità preposta.

Riassumendo, il formato p7m risulta essere, quindi, una specie di involucro (una busta crittografata) che al suo interno contiene un documento che può essere indistintamente di qualsiasi tipo: pdf, exe, tiff, gif, png, doc, vbs, xls, odt, etc.

In modo inverso, quando l'utente si pone in qualità di destinatario del documento stesso, al suo ricevimento lo troverà firmato, imbustato e crittografato, e dovrà fare alcune operazioni per sapere se il file è originale e integro, o se è stato manomesso in un qualunque momento dopo la sua spedizione. Il principio consiste nell'estrarre il file originale e creare una nuova impronta, che poi verrà confrontata con quella criptata contenuta nella busta: se le due impronte coincidono, il file non è stato manomesso ed è perfettamente integro.

In sintesi:

1. Estrazione del file originale dalla busta;
2. Creazione di un'impronta attraverso l'applicazione dell'algoritmo SHA-1;
3. Estrazione dell'impronta criptata con la chiave pubblica, anch'essa contenuta nella busta;
4. Confronto delle due impronte.

Dopo l'apertura del documento, quindi, seguirà la verifica della firma presente sul documento (che può essere una o più di una); il programma deve fornire l'opportunità di verificare che il certificato di firma non sia scaduto, ma che sia ancora valido, ottenendo così le informazioni sul nome del firmatario, le due date di inizio e fine validità, per le quali dovremmo verificare che l'attuale data sia ivi compresa. A questo punto però mancherebbe ancora il controllo presso la CA, che garantisce definitivamente che il certificato in questione non sia divenuto inattendibile, nei casi che ricoprono la denuncia di furto/smarrimento del dispositivo di firma, la scadenza naturale o altri eventi accidentali.

Firma Multipla

Per quanto riguarda l'apposizione della firma digitale multipla, vige la regola che:

1. Una stessa busta crittografica può contenere più firme digitali, che vanno suddivise in:

- ☐ «Firme parallele», quando il sottoscrittore, utilizzando la propria chiave privata, firma solo i dati contenuti nella busta stessa;
- ☐ «Controfirme», quando il sottoscrittore, utilizzando la propria chiave privata, firma una precedente firma apposta da altro sottoscrittore.

2. Il formato delle firme multiple e' uno dei tre formati ammessi;
3. L'apposizione di firme multiple non comporta l'applicazione di ulteriori estensioni al file firmato, oltre alla prima.

Continuando a discutere nell'ambito delle firme multiple, si ricorda, però, come una busta crittografica possa contenere, al suo interno, a sua volta altre buste crittografiche (quindi firmate) ed in tal caso venga applicata un'ulteriore estensione .p7m; per cui si evidenziano tre diversi tipi di firma multipla:

- *Firma multipla a catena* ovvero la firma viene applicata ad un documento informatico (Art.12, comma 6)
- *Firma multipla parallela* ovvero si ha un'unica busta crittografica .p7m che contiene le firme riferite allo stesso documento elettronico (Deliberazione CNIPA 4/2005 Art.13, comma 1, lettera a).
- *Firma multipla controfirma* ovvero si ha un'unica busta crittografica .p7m che contiene la prima firma riferita al documento elettronico e le successive firme applicate alla firma del precedente firmatario (Deliberazione CNIPA 4/2005 Art.13, comma 1, lettera b).

Con una rapida analisi si giunge alla conclusione che la firma multipla a catena sia poco pratica, poiché ad ogni firma viene aggiunta un'estensione .p7m, dando origine a dei file che in pochi passaggi acquisiscono una estensione spropositata (un "documento.doc" con 4 firme diventerà "documento.doc.p7m.p7m.p7m.p7m") e dovrà essere verificato 4 volte, ogni volta salvando il file risultante dalla verifica; nel tipo di firma multipla parallela, invece, succede che l'estensione .p7m rimane una ma, ad esempio, l'uso di programmi di verifica che non mostrano dettagli sul "momento" in cui sono state apposte le firme, e magari associati ad un utente con non troppa esperienza in materia, fanno sì che questo tipo di firma possa generare dubbi (l'ordine delle firme, ad esempio, non e' cronologico ma alfabetico, generando così parecchia confusione su chi abbia firmato cosa e quando). Si deduce che, nel formato P7M, per ogni firma apposta ad un documento venga generata una nuova busta crittografata attorno al documento, che porta al risultato di ottenere una "matrioska" di firme che implica una notevole complessità nel ripercorrere il processo contrario in fase di verifica.

Vantaggi & Svantaggi

Si apprende ora come sia inevitabile che, proprio essendo uno standard in uso ormai da lungo tempo, esso cominci ad essere ormai vetusto e certamente porti con sé lo svantaggio di poter essere utilizzato solo se si è in possesso di un software opportuno, che permetta di leggere i documenti salvati e firmati secondo tale formato; infatti gli utilizzatori, siano essi mittenti o destinatari, devono entrambi essere dotati di un apposito programma che risulta essere sempre più spesso un software altamente sofisticato, con un'immensa lista di opzioni da combinarsi in svariati modi, al punto che il suo utilizzo risulta oggettivamente complicato alla maggior parte degli utenti, fatto salvo l'eccezione di qualche raro esperto.
Si può affermare con certezza che l'inviolabilità dei certificati e dalla chiave privata è assicurata dalle autorità citate precedentemente, preposte al rilascio dei certificati per firma digitale, le quali installano questi ultimi su supporti che non possono essere contraffatti o alterati. Questi supporti sono smart card o token USB. L'operazione di criptaggio dell'impronta, ovvero la firma digitale vera e propria, avviene a bordo di questi supporti: il programma dopo aver estratto l'impronta la invia al supporto che applica la chiave privata e restituisce l'impronta firmata. Il supporto si comporta come una cassaforte intelligente, che non permette l'uscita dei suoi valori, ma è in grado di operare al suo interno.

Certamente il PKCS#7 rimane un formato sicuro ed efficiente, ed mantiene la comodità per cui con una stessa coppia di chiavi – pubblica e privata - si possono gestire varie coppie di interlocutori, ma non va dimenticato, a suo discapito, che il calcolo crittografico è davvero molto oneroso, con elevatissimi tempi di calcolo. Da non sottovalutare nemmeno la delicatezza del momento della distribuzione della chiave pubblica ai vari utenti, i quali la andranno ad utilizzare per poter leggere il documento ricevuto e verificarne l'autenticità. Infine, il documento elettronico apparirà inevitabilmente pesante poiché, per come viene strutturato, il file firmato viene spedito dentro ad una busta di trasporto che reca le informazioni crittografiche, rese necessarie dal processo di firma.

2.6.4.2. Firma digitale in formato PDF

Legislazione

Questo nuovo formato di firma è nato dall'esigenza di garantire una maggiore efficienza e di poter sfruttare ancora meglio i mezzi informatici nella gestione elettronica dei documenti. Con queste premesse si giunge a questa analisi, dove si esplorerà il formato di firma PDF, che è il secondo formato di firma digitale con pieno valore legale valido in Italia, tanto da essere anche uno standard ISO (ISO/IEC 19005). Il formato PDF è stato riconosciuto pienamente valido per la firma digitale ai sensi dell'Art.12, comma 9, della Deliberazione CNIPA 4/2005 mediante la stipula di un

Protocollo d'Intesa sottoscritto definitivamente il 16 Febbraio 2006 dal CNIPA e da Adobe System Inc.

Il formato .pdf fa il suo esordio nel campo informatico parecchi anni fa e si mostra come un semplice formato documentale indipendente dalla piattaforma hardware in uso e stampabile ad alta qualità, ma con il tempo si è evoluto in un formato "intelligente" capace di rappresentare non solo testo e grafica ma anche dati, metadati e logica applicativa, con varie funzioni di sicurezza che ne consentono il controllo e ne accrescono l'affidabilità.

Modo d'Uso

I passi fondamentali per apporre la firma di tipo PDF, sia con Adobe Acrobat che con Acrobat Reader, sono molto simili e si possono sintetizzare come segue:

1. Apporre la firma: dopo l'apertura del documento con Acrobat Reader, si clicca sulla funzione apposita;
2. Uso della smart Card: il suo inserimento ci consente di tracciare sul documento il riquadro che conterrà la firma;
3. Scelta del certificato di firma: si seleziona il certificato desiderato e lo si convalida con la digitazione del PIN, e il file viene definitivamente firmato e salvato.

Per la verifica della firme apposte, ci si comporta nel seguente modo:

1. Localizzazione firme: si individuano dove e quali sono le firme contenute nel documento;
2. Verifica: il programma ci consente di verificare, per ogni firma apposta, che il documento non sia stato modificato dopo la firma, che il certificato del sottoscrittore sia garantito da una CA, che lo stesso non sia scaduto, né sospeso o revocato;

Dal punto di vista operativo, l'uso di questo formato è assai semplice, poiché per utilizzare la firma digitale è necessario creare un file "Digital ID" che potrà essere usato per firmare i documenti veri e propri, e un certificato di verifica che servirà per controllarne l'autenticità e che verrà incluso nel documento PDF firmato: si tratta di un file creato dall'utente e che, una volta in possesso di terzi, consente loro di verificare l'autenticità della firma digitale dell'utente contenuta nei documenti PDF. Solitamente tale Digital ID viene legato ad un dispositivo hardware, ad esempio una smart card: in questo modo solo chi ha la smart card potrà usare il Digital ID per firmare i file PDF. Firmare digitalmente un PDF è possibile solo se esso contiene l'apposito campo dedicato alla firma digitale, campo che si può creare solo con Adobe Acrobat Standard/Professional e con pochi altri software professionali come Form Router o PDF Signator. In sostanza, coloro i quali intendessero sottoscrivere documenti con il formato PDF, si troverebbero ad utilizzare il consueto kit di firma digitale e le stesse procedure, già viste nel precedente paragrafo, per cui userebbero il kit

precedentemente fornitogli dal proprio certificatore di riferimento ed un qualsiasi prodotto di elaborazione PDF, purché esso generi file sottoscritti conformemente alle specifiche del formato stesso.

Va precisato che, seppur simili, non vanno confusi i concetti di file con estensione .pdf, il software Acrobat della ditta Adobe e il formato di firma PDF. A tal proposito specifichiamo che al momento esistono già alcuni tool open source che sono in grado di apporre la firma secondo il formato PDF. Ma il software chiamato Adobe Acrobat ha funzioni ben più numerose e produttive rispetto i programmi similari, anche solo per quanto riguarda la sola firma digitale. In ogni caso, anche con il software gratuito Adobe Reader è possibile, ma solo in determinate condizioni, apporre firme digitali e marche temporali, oltre che verificarle, senza gravare di alcun onere economico il firmatario. Questa possibilità è data dalla tecnologia di altri software, come Adobe Reader Extensions, il quale, non essendo uno shareware dalla rete, comporta un costo per colui che attiva il documento da firmare, mentre se si usa un'altra soluzione che è quella data dall'uso del software chiamato Adobe Reader si rimane assolutamente a costo zero, purché con lo stesso programma si eseguano sia la compilazione che la firma. Permane, invece, il costo zero per l'utente che riceve il file e deve solo verificare la firma e leggerne il contenuto, e lo può fare comodamente con il ben noto Acrobat Reader. Come già visto nel primo formato, anche in questo caso il processo di firma è strettamente collegato ad un processo di crittografia, che per questa tipologia di firma adotta una combinazione degli algoritmi RC4 ed MD5 (Message-Digest algorithm 5) che sono tra i più usati per garantire l'integrità dei file tramite un hash a 128 bit.

Firme Multiple

Per quanto riguarda il caso delle firme multiple, esse sono possibili purché il creatore del documento abbia inserito i necessari "diritti" per poterlo fare, sempre all'interno dello stesso software che si chiama Reader Extension: solo rispettando queste premesse, il formato PDF consente di apporre firme digitali multiple, viste come sigilli alle revisioni o alle nuove versioni di un documento. Vi è, perciò, la possibilità di apportare modifiche al documento anche se queste dovessero essere successive alla firma, senza però incorrere nel problema di invalidare la firma stessa. Questa funzionalità, non disponibile con il formato P7M, sfrutta la caratteristica del PDF di effettuare il salvataggio incrementale dei dati ed è fondamentale quando la firma è utilizzata in processi in cui più persone collaborano ad un unico documento modificandolo e apponendovi la propria firma digitale in tempi successivi. Un ambito in cui questa caratteristica è indispensabile è quello della modulistica elettronica, dove i vari processi tipicamente prevedono che più persone interagiscano con lo stesso documento, aggiungendo e sottoscrivendo i propri dati in tempi successivi (come spesso capita anche in ambito medico-clinico, si vedano referti e similari). Da notare che i campi firma consentono di contestualizzare la validità della firma a sezioni differenti di

un documento, cioè che più persone possono sottoscrivere parti diverse di un unico documento, dando una chiara percezione di cosa ciascuno abbia sottoscritto, esattamente come avviene con la carta.

Con il formato PDF le firme multiple sono gestite in modo trasparente per l'utente, il quale le ritrova tutte elencate in ordine di apposizione cronologica in un unico pannello firme di facile lettura nell'unico file PDF, fruibile nello stesso identico modo di un PDF non firmato. È possibile, inoltre, verificare tutte queste firme con Acrobat Reader, senza alcun costo e senza alcuna difficoltà anche per l'utente che ignori i meccanismi della firma digitale. Da un punto di vista operativo permangono alcune perplessità sull'uso di numerose firme multiple nel modello PDF.

Vantaggi & Svantaggi

Questo formato di firma ha il vantaggio immediato che, sia le specifiche del formato che il visualizzatore stesso, siano disponibili e gratuiti, anche direttamente dal web. Infatti, la gestione degli applicativi già sviluppati ed esistenti a tale scopo, non obbliga al pagamento di alcuna "royalty" ad alcun soggetto. Grazie a ciò, questo tipo di firma ha già ottenuto una larga diffusione e parecchio consenso tra gli utenti, insieme ad un'immediata fruibilità, ed inoltre risponde, senza dubbio, ai requisiti tecnici e giuridici per poter trasportare firme digitali al suo interno.
Nel caso si usi la firma digitale nativa nel formato PDF, essa si trova ad offrire un'ampia serie di caratteristiche vantaggiose non ancora presenti in altri prodotti software simili, già disponibili sul mercato. Tali prodotti similari, infatti, utilizzano generalmente una busta PKCS#7 di tipo "signed and enveloped data" (formato .p7m), un formato caratterizzato da numerose limitazioni d'uso. Nel precedente formato, inoltre, tuttora molti utenti possano trovare difficoltà nel reperire un'applicazione di verifica di file con firma digitale P7M. Al contrario, la stragrande maggioranza degli utenti di personal computer (circa il 90% secondo le stime più recenti) sono in grado di riconoscere un file PDF e di utilizzare il visualizzatore Adobe Reader gratuito, ottenendo implicitamente la possibilità di verificare le eventuali firme digitali in esso contenute.
Da sottolineare, invece, il fatto che il documento PDF con firma digitale PDF non subisce alcuna trasformazione in altro formato diverso da sé stesso e quindi esso offre in definitiva funzionalità di firma digitale trasparenti rispetto all'esigenza primaria di accedere con facilità ai documenti firmati.
Ultimo, ma non per importanza, la soluzione PDF consente di realizzare una piena interoperabilità tra i servizi di marcatura temporale offerti dai diversi certificatori, eliminando l'onere a carico degli utenti di dotarsi di differenti prodotti di verifica, a seconda delle diverse tipologie di formati in uso.

Analogamente a quanto già visto nel formato P7M, anche nel formato PDF la firma comporta un aumento del "peso" del documento rispetto quello iniziale ancora da firmare. Va specificato, per meglio comprendere il concetto, che le firme digitali in un PDF possono essere visibili o invisibili: le

prime appaiono come immagini nel documento, e possono rappresentare la propria firma reale su carta, un timbro, un logo e così via a scelta di chi ha creato la firma digitale stessa. Le seconde, invece, non appaiono sul documento, ma sono verificabili con la stessa procedura di quelle visibili ed hanno lo stesso valore. Quindi, per chiarezza, mentre una firma di file inclusi in una busta PKCS#7 comporta l'aggiunta al file originario di circa 4 Kbyte, per la firma in un file PDF vengono aggiunti almeno 16 Kbyte (per la firma invisibile) più un ulteriore carico (se si utilizza la firma visibile), che varia in funzione della risoluzione e dei colori impiegati. In casi estremi, il "peso" del documento può dunque aumentare di diverse centinaia di Kbyte.

Altro punto critico su cui far attenzione è la differenza tra l'apposizione della marca temporale e la funzione del programma detta "SigningTime": la prima e' il vero riferimento temporale opponibile a terzi, mentre la seconda è solamente una funzione del software che permette di aggiungere al documento un riferimento temporale basato sulla data e ora del computer, inaffidabile e non valido ai fini dell'opponibilità a terzi e della validità nel tempo quando il certificato di firma usato sarà scaduto.

Purtroppo va ricordato che anche con questo formato si potrebbero riscontrare problemi non banali, nell'uso di set di font differenti tra mittente e destinatario del documento, tra firmatario e lettore. I problemi potrebbero insorgere con i font inclusi (o esclusi) nel file firmato, o meglio, nella rappresentazione di quanto firmato, in quanto si suppone che la stabilità e la validità della firma siano indipendenti dalla piattaforma e dall'applicazione di origine. Non sempre il programma supporta pienamente set di caratteri diversi, come può facilmente succedere tra i caratteri europei e quelli orientali, o ancor più facilmente tra le lingue con caratteri accentati e lingue senza, come può usualmente succedere se il destinatario e il mittente appartengono a idiomi e piattaforme diverse.

Da sapere, inoltre, che un qualunque file in formato PDF non può sostenere automaticamente la firma digitale; solo quando la firma è supportata nativamente il visualizzatore (Adobe Reader) identifica, segnala e addirittura può evitare all'utente ogni eventuale alterazione successiva alla verifica di una firma digitale; tutto ciò per arrivare a dire che per l'apposizione della firma digitale nativa in PDF esistono alcune limitazioni in merito ai contenuti:

- I contenuti audio e video non sono consentiti;
- JavaScript e avvio di file eseguibili non sono consentiti;
- Tutti i font devono essere inclusi nel file e devono essere legalmente includibili per uso universale;
- I colori devono essere definiti in modalità indipendente dal dispositivo;
- La crittografia non è consentita.

Come nota finale, va segnalato che per poter scambiare documenti PDF firmati con una Pubblica Amministrazione è necessario che essa comunichi ufficialmente tale possibilità, anche sul proprio sito web, altrimenti lo scambio di dati risulterebbe impossibile.

2.6.4.3. Firma digitale in formato XML

Legislazione

XML è un nuovo standard promosso dal World Wide Web Consortium (W3C) e si affianca al linguaggio di programmazione omonimo, con la produzione di un framework che deve attuare lo standard W3C "XML Signature Syntax and Processing (XMLDsig)".
Queste tecnologie sono gestite dal consorzio W3C, responsabile della definizione e divulgazione di un insieme specifico di regole, linee guida e convenzioni per la creazione di file che possano essere generati ed elaborati in modo semplice da computer e applicazioni diversi.

Il linguaggio di programmazione XML risulta essere uno strumento già da tempo diffuso soprattutto per la strutturazione e lo scambio di dati, e per questo usato ormai da parecchio tempo in numerosi contesti, tanto che con il esso sono già prodotti i documenti elettronici di tipo sanitario e finanziario (come il corporate banking). E' stato pertanto un passo obbligato quello di considerare e rendere legale un nuovo formato di firma digitale, che consentisse di sfruttare la potenzialità e la flessibilità di questo linguaggio. Nel caso dell'Italia questo terzo formato di firma è l'ultimo standard approvato, ed è entrato in vigore con la delibera CNIPA in data del 18 maggio 2006 (Deliberazione n. 34/06).

Modi d'Uso

Dal lato pratico, se si volesse creare una firma XML per un qualsiasi contenuto digitale si dovrebbero percorrere i seguenti passaggi:

1. Ottenere il digest: cioè calcolare il valore di digest per ciascun oggetto che va firmato;
2. Acquisire il manifest: mettere in un elemento che funge da raccoglitore (manifest, appunto) l'insieme dei digest ottenuti e altre informazioni contestuali alla struttura (i puntatori alle risorse URI ad esempio);
3. Firmare il digest: si genera il valore digest del manifest e solo ora il digest viene definitivamente firmato con la chiave privata.

In un momento successivo, per procedere alla verifica o validazione della firma apposta su di un documento XML, sono previsti due passi:

1. Validazione della firma stessa: ci si assicura dell'integrità del valore di digest dell'intero elemento firmato (del manifest);
2. Validazione del digest: ovvero la validazione del valore digest di ogni singolo dato.

Dalla struttura necessaria nel processo di firma si deduce come, attraverso il manifest e la canonizzazione, la firma possa essere applicata contemporaneamente al contenuto di una o più risorse, da cui si può evincere facilmente una delle principali caratteristiche di questo formato di firma. Infatti, una caratteristica fondamentale di una firma XML è la capacità di poter firmare solo una porzione specifica di un albero XML, invece dell'intero documento. Questo può risultare utile quando un documento XML ha una lunga storia, nella quale componenti diverse sono state aggiunte da autori diversi in tempi diversi, e si abbia la necessità di firmare solo certi elementi rilevanti.

Questa flessibilità è anche critica in situazioni dove sia importante assicurare l'integrità di certe porzioni di un documento XML, lasciando aperta la possibilità di effettuare modifiche su altre porzioni del documento. Si consideri, per esempio, un modulo XML firmato e inviato ad un utente perché lo completi. Se la firma si estendesse sul modulo completo, ogni modifica dell'utente invaliderebbe la firma originaria. In sintesi, il formato XML ci dà due enormi vantaggi rispetto i precedenti formati, esattamente permettendoci di firmare solo alcune parti di un documento, e non per forza la sua totalità, e conseguentemente di poter fare delle aggiunte al documento in fasi successive alla prima firma, e contemporaneamente di avere molteplici autori nello stesso documento, ognuno dei quali firma la parte di propria competenza.

Analogamente ai precedenti formati, per il suo utilizzo sono sufficienti due dispositivi che ormai sono ben noti e sono sicuri per la generazione delle firme (una smartcard o un token USB) e un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso; purtroppo ancora non e' stata garantita la possibilità di eterogeneità tra dispositivi differenti (dispositivo fornito dal certificatore A da usare con il software di firma fornito dal certificatore B, e viceversa).

Firme multiple

Per quanto riguarda il possibile utilizzo delle firme multiple, esse sono ammesse e possono essere di tipo congiunto, detto anche parallelo, e caratterizzate dal fatto che sono apposte in modo indipendente l'una dall'altra sugli stessi dati di partenza.

L'unico accorgimento da tener a memoria è che, se la busta di partenza contenesse una firma XML in modalità *detached*, le firme seguenti dovrebbero essere apposte utilizzando ancora la modalità *detached,* facendo riferimento ai dati referenziati dal primo firmatario. Analogamente, se la busta crittografica di partenza contenesse una firma XML in modalità *enveloped*, le firme seguenti andrebbero apposte utilizzando ancora la modalità *enveloped*. Le controFirme rimangono valide come nel caso del PDF.

Vantaggi & Svantaggi

Il W3C sostiene che lo standard ultimo emesso ha due vantaggi sostanziali rispetto alle soluzioni proprietarie già viste in circolazione: può essere implementato attraverso gli stessi strumenti di sviluppo che già ampiamente si utilizzano per costruire applicazioni XML e permette agli utenti di firmare anche solo alcune parti di un documento.
Per definizione dello stesso linguaggio XML, da cui deriva la firma omonima, esso possiede un'assoluta dinamicità e flessibilità e questo fa sì che due documenti XML possano essere *logicamente* equivalenti, ma possano altresì essere fondamentalmente differenti, ad es., a causa di una diversa spaziatura all'interno dei tag, dei delimitatori di linea, dei commenti e così via: ciò non intacca la sostanza del documento ma ne altera profondamente la forma, rendendoli pertanto due documenti completamente diversi, se non nella sostanza, almeno nella forma.
Le applicazioni XML tendono ad ignorare quelle differenze, perché non hanno impatto sull'informazione in sé, ma tutto ciò e' fondamentale per le firme digitali, perché la validazione di una firma digitale dovrebbe essere applicata esattamente sullo stesso flusso di byte di quando è stata generata. Per risolvere questo problema, è stato introdotto il concetto di canonizzazione dei documenti XML (XML-C14N), che ha la funzione di convertire un documento XML nella sua forma canonica, appunto, cioè nell'applicare un insieme di trasformazioni in modo che rappresentino tutte le informazioni variabili in maniera standard, affinché due documenti logicamente equivalenti abbiano esattamente la stessa forma canonica. Questo passaggio sottopone il documento ad una elaborazione che riesce ad estrarre un riassunto univoco, associabile ad un impronta altrettanto univoca del documento stesso, in modo tale da essere al riparo da qualsiasi fastidio di incompatibilità nella firma.
Ricordiamo qui che esistono tre diversi tipi di firma XML:

- *Enveloping signature*: quando la firma contiene l'oggetto firmato;
- *Enveloped signature*: quando l'oggetto firmato contiene la firma;
- *Detached signature*: quando l'oggetto firmato non è incluso nell'elemento di firma.

Come precedentemente già discusso per i primi due formati di firma, anche in questo terzo formato si ricorre all'uso del digest. Sapendo che la funzione utilizzata per calcolarne il valore è molto sensibile alle variazioni del documento e quindi al fine di garantire il corretto funzionamento del meccanismo della firma digitale, il digest deve essere generato utilizzando la forma canonica del documento XML, cioè, prima di ricavarne il digest, il documento subisce il processo di canonizzazione, che rende lo stesso omogeneo rispetto agli altri simili, secondo una serie di regole già stilate. Inoltre per la validazione di una firma è necessario anche che il dato firmato sia accessibile, ovvero che il riferimento della locazione dell'oggetto firmato sia indicato nella firma XML stessa per mezzo di un opportuno URI (Uniform Resource Identifier).
Ancora una volta, il meccanismo usato è quello dei sistemi a chiave asimmetrica, dove ritroviamo due chiavi tra loro correlate: una privata (segreta) e una pubblica (divulgabile). In questo modo, per poter proteggere i documenti, ogni codifica effettuata con chiave privata può essere decodificata unicamente con chiave pubblica; in questo modo ho la sicurezza che solo determinate persone potranno decodificare i dati inviati.
Fino ad ora, i precedenti metodi affiancano l'uso della chiave asimmetrica a quello del SSL (Secure Socket Layer) che consente di creare un canale protetto e sicuro ai fini dello scambio di dati tra due diverse applicazioni. Però questa tecnologia non è basata sulla protezione di singole parti di un documento, bensì sulla cifratura dell'intero documento che viene così ben protetto durante lo scambio, ma arrivato a destinazione durante la decifratura dell'oggetto, esso diviene vulnerabile.

Nel piano dell' XML, data la sua enorme flessibilità, si predilige la modularità e quindi il fatto di poter firmare anche solo una singola parte del documento e non la sua interezza; per questo XML affronta il problema della sicurezza attraverso XML Encryption, che è un software in grado di protegger l'intero documento, o solo alcune sue parti, permettendone di criptare gli elementi attraverso i comuni algoritmi di crittografia. A differenza di tecnologie simili, XML Encryption dà la possibilità di cifrare la chiave di codifica; in pratica, la chiave per codificare il dato viene trasmessa, anch'essa cifrata, insieme al dato protetto all'interno del documento XML.
È possibile, quindi, utilizzare la crittografia XML per sostituire qualsiasi elemento o documento XML con un elemento contenente i dati XML crittografati. Tale elemento può contenere anche sottoelementi che includono informazioni sulle chiavi e i processi utilizzati durante la crittografia. La crittografia XML consente di inserire più elementi crittografati all'interno di un documento e di crittografare un elemento più volte.
Al fine di metter in luce un altro vantaggio di questo formato di firma, facendo un paragone con le firme digitali non XML (come ad esempio quelle in formato PKCS), le firme XML aggiungono al dato firmato le caratteristiche d'identificazione e di integrità. Tuttavia, a differenza delle firme non XML, queste sono state progettate per trarre vantaggio delle caratteristiche dei protocolli Internet e del linguaggio XML: infatti, una firma digitale XML è una firma che può essere usata in transazioni XML. Lo standard definisce uno schema per il formato di una firma digitale applicata su un dato in formato

arbitrario (ma spesso XML). Questo ancora a riprova dell'estrema flessibilità di questo linguaggio/formato, che bene si integra nei processi che coinvolgono la rete. Con queste premesse si deduce come l'uso del formato XML faciliterà lo sviluppo di innovative applicazioni in ambito sanitario, nel colloquio tra la Pubblica Amministrazione e le aziende, ed in futuro nell'erogazione di servizi sempre più evoluti, atti a soddisfare le esigenze del cittadino.

Risulta lampante come con questo formato sia possibile introdurre, in modo poco invasivo, la firma digitale in settori come quello bancario e sanitario, poiché il linguaggio in questione ha notevole rilevanza nella gestione elettronica dei flussi documentali, dato che questo metodo usa lo stesso linguaggio con cui sono scritti i siti internet, e perciò può essere implementato attraverso gli stessi strumenti di sviluppo che già si utilizzano per costruire applicazioni XML. Per lo stesso motivo questo linguaggio si ritrova ad usare gli stessi standard HL7 già utilizzati in vari ambiti della sanità, oppure di poter creare in modo molto veloce dei documenti firmati che risultino allo stesso tempo leggeri. Ciò garantisce una grande interoperabilità con i messaggi prodotti da altri applicativi, grazie alla massiva standardizzazione ottenuta con l'utilizzo del protocollo HL7.
Per aumentare la sicurezza, il formato XML, contrariamente agli altri formati, prevede che in caso di firma digitale con procedure automatiche, ad esempio per la sottoscrizione di un elevato numero di documenti, si possa proseguire secondo la prassi consueta e sia sufficiente ricorrere unicamente ad una nuova coppia di chiavi per l'identificazione, diversa da tutte le altre, usate per la sottoscrizione di documenti singoli. Il processo così rimane molto più agile e snello rispetto a quello adottato dagli altri due metodi, e da come risultato un documento molto leggero.
Per aumentare il livello di sicurezza, questo formato ha abbandonato l'uso dello standard S/MIME, per lasciar spazio all'utilizzo di altri due prodotti di W3C e questo sebbene non siano passati molti anni dalla nascita di questo formato; si è sentita comunque la necessità di adottare altri programmi complementari, quali "XML Encryption", per la crittografia di parti di un documento, "XML Key Management", per la gestione delle chiavi crittografiche e "XML Signature", per la firma.

Questi nuovi programmi portano ad un altro passo fondamentale ed esclusivo di questo formato, ovvero il fatto di ottenere l'indipendenza rispetto alla modalità di trasmissione dei documenti, il che significa che un documento firmato con XML Signature e criptato con XML Encryption può essere spedito per posta elettronica o scaricato via http o FTP, mentre S/MIME è utilizzabile soltanto con SMTP. Anche in questo caso, la scelta degli standard basati su XML ha permesso di adattare, in modo rapido e disinvolto, quanto già creato ad eventuali scelte future di cambiamento dell'architettura del progetto. Invece, S/MIME è fortemente orientato verso la posta elettronica ed un simile cambiamento costringerebbe a riscrivere interamente le funzioni che firmano e cifrano i dati in modo da supportare uno standard più consono al protocollo in uso.
Se andiamo ad analizzare il peso dei file firmati, osserviamo che gli algoritmi per la crittografia e la firma sono di due tipi, *Base* (fornisce chiavi brevi e algoritmi leggeri) e *Avanzato* (con chiavi più

lunghe e algoritmi più sicuri), e a seconda del tipo usato, otteniamo rispettivamente che la lunghezza della chiave ottenuta sia almeno 512 bit per la firma e altri 40 bit per la crittografia nel primo caso, mentre sono almeno 1024 bit più altri 168 bit per la crittografia nel secondo caso. Ne risultano delle firme tutto sommato leggere e agili dal punto di vista computazionale.

Come ulteriore, nonché finale, considerazione, si nota che la scelta di utilizzare XML e le tecnologie ad esso correlate permetta di abbassare la soglia tecnologica richiesta alle PMI e renda più semplice l'interoperabilità con i sistemi informativi aziendali più complessi, come le grandi Pubbliche Amministrazioni. Questa semplicità nell'operare su documenti XML si traduce, oltretutto, nella possibilità di generare strumenti efficaci e sicuri sia per gli utilizzatori finali che per il team di sviluppo del progetto. Il risultato è, dunque, la definizione e realizzazione di una piattaforma comune per la comunicazione di informazioni di vario tipo, che permetterà alle aziende di interoperare senza modificare in modo sensibile i propri sistemi operativi.

Per ora l'unica nota non positiva sembra essere il fatto che, purtroppo, al momento non è ancora il metodo più diffuso, ma è di buon auspicio che molti colossi del settore informatico si siano già impegnati nella produzione di software per la gestione di questo formato di firma, lasciando presagire che XML rimanga il formato che possiede le maggiori caratteristiche di flessibilità, senza intaccare le rigide esigenze della firma digitale.

2.6.5. *Certificati, Certification Authority, Registration Authority Registration Authority*

Si è precedentemente visto che un ruolo importantissimo nella dematerializzazione viene rivestito dalla Certification Authority - CA, soprattutto nella gestione della vita dei certificati di firma. Molto spesso può essere utile affiancare alla CA anche un organismo organizzativo (Registration Authority - RA), interno alla Struttura Sanitaria, il quale gestisca le attività di emissione dei dispositivi di firma e di sospensione/revoca dei certificati associati. Questo approccio organizzativo può risultare molto vantaggioso in quanto l'ambito di utilizzo dei dispositivi di firma è ben preciso e indissolubilmente legato al rapporto contrattuale fra l'operatore (sia esso un medico, un ausiliario, un amministrativo, etc.) firmatario e la Struttura Sanitaria. Inoltre, il datore di lavoro può unilateralmente revocare o sospendere l'uso delle smart card di un soggetto all'interno della propria struttura, così come, in base all'art.32, co.3, il Certificatore che rilascia i certificati qualificati di firma deve "procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo". Molto spesso, ove si è proceduto all'istituzione di una RA interna alla Struttura Sanitaria, ci si è appoggiati operativamente alle unità dei Sistemi Informativi o dell'Ufficio Personale, i quali hanno gestito in modo parallelo sia il badge personale che il dispositivo di autenticazione, che quello

di firma. Dal punto di vista della sicurezza, la presenza di una RA all'interno della Struttura Sanitaria rappresenta un notevole valore aggiunto per permettere di ottenere tempestive revoche/sospensioni dei certificati di firma/autenticazione, ma soprattutto immediate revoche/sospensioni del potere di firma, che verrà illustrato e quindi compreso più avanti. Per meglio capire questo punto, basti pensare ad un medico, appartenente ad una determinata Struttura Sanitaria e titolare di un certificato di firma emesso da una CA a livello Regionale, il quale si trasferisca in un'altra Struttura della stessa Regione: il certificato di firma rimarrà comunque valido anche dopo il trasferimento, ma il potere di firma dovrà assolutamente essergli revocato nella prima Struttura ed eventualmente attivato presso la seconda.

2.7. CLASSIFICAZIONE, FASCICOLAZIONE E SCARTO DEI DOCUMENTI

2.7.1. *Classificazione e fascicolazione*

La Guida elaborata dal Comitato sugli archivi elettronici del Consiglio internazionale degli archivi e anche il Codice dell'Amministrazione Digitale sostengono come fondamentale il mantenimento dell'autenticità, della leggibilità e intelligibilità nel tempo della documentazione digitale prodotta, anche ai fini della funzione conservativa di essa.
L'integrità e l'identificazione univoca e certa dei documenti e di ogni relazione tra di essi costituiscono gli elementi indispensabili per garantire la reperibilità del documento da rinvenire un domani, oltre che la certezza della sua validità giuridica e la totale rispondenza al criterio di ricerca. Pertanto è necessario da subito porre la propria attenzione sui dati ritenuti importanti per esprimere l'appartenenza del singolo documento al complesso archivistico (fascicolo, serie, fondo, ecc.) al quale esso organicamente e gerarchicamente appartiene. Si afferma che fin dall'inizio le regole vanno poste: già ben prima della creazione del singolo documento debbono essere studiate e rinvenute le policy di strutturazione dell'archivio ed in base ad esse al momento della nascita il documento deve riportare gli elementi archivistici ritenuti necessari.
E' stato ormai ampiamente dimostrato dagli studiosi di questo specifico settore, che certe informazioni archivistiche debbano necessariamente essere inserite in modo corretto in un corpus strutturato di documenti, pena l'incertezza su autenticità, validità, rinvenimento sicuro e veloce di dati e documenti. Dalle analisi effettuate, in ogni ambito applicativo sono stati indicati gli elementi essenziali all'archiviazione: ad esempio, per i referti di Laboratorio sono stati individuati come minimo l'identificazione del paziente, l'indirizzo, la destinazione del referto, il richiedente. Essi, di fatto, possono rimandare a fonti e documenti di tipo diverso, ma facenti parte del medesimo fascicolo virtuale (come la richiesta di prestazione redatta dal Medico di Medicina Generale - MMG).

Risulta necessario, inoltre, che i documenti restino identificabili in maniera univoca attraverso elementi e attributi ad essi relativi, quali per esempio:

- i dati di provenienza (organizzazione responsabile/autore);
- le componenti logiche interne;
- la registrazione univoca e con data certa, che testimoni in modo incontrovertibile l'avvenuta acquisizione all'archivio;
- le relazioni documentarie che identificano le modalità di accumulazione, formazione e organizzazione stabile dell'archivio (classificazione e fascicolazione, accessibilità, tempi di conservazione, procedure di riversamento e di validazione e relative responsabilità). Il documento, quindi, sembra dover essere autoconsistente e il suo profilo dovrà contenere tutte le informazioni necessarie a garantire la sua conservazione in forma autentica e contestualizzata, mediante anche l'aggiunta di informazioni relative ai livelli superiori, cioè alla struttura archivistica alla quale lo stesso documento è destinato ad appartenere in maniera definitiva nel passaggio all'archivio storico, che nel mondo informatico è rappresentato dalla conservazione sostitutiva.

In altre parole appare importante far uso degli strumenti e delle pratiche solitamente riservate alla corretta strutturazione degli archivi, quali i titolari, i massimari di scarto, i repertori dei fascicoli, i regolamenti. Si tratta peraltro di strumenti e pratiche che in ambito sanitario sono state parecchio trascurate, con conseguenti danni, anche gravi, per la conservazione permanente della documentazione e del suo reperimento. Già il D.lgs n.445/2000, Testo Unico sulla documentazione amministrativa, e ora ancor di più il Codice dell'Amministrazione Digitale, richiamano l'obbligo delle pubbliche amministrazioni di dotarsi di questi strumenti nella costituzione e gestione di un archivio.
E' indispensabile analizzare e poi progettare adeguatamente la conservazione di un documento in ambiente digitale, dal momento della sua creazione fino alla sua acquisizione all'archivio, che coincide con la sua assunzione al protocollo, o, per i documenti non soggetti a protocollazione, con l'attribuzione di una classifica che identifica a quale segmento di procedura della Struttura il documento stesso venga attribuito.
Va inoltre sottolineato che l'attività clinico-sanitaria, seppur avente finalità di diagnosi, cura, terapia, prevenzione, ecc, si debba basare su una complessa attività amministrativa, che operi attraverso una molteplicità di procedure tali da investire un settore cruciale qual è quello della salute del cittadino. La gestione documentale, sia essa di carattere sanitario oppure amministrativo, deve essere affrontata con strumenti omogenei all'interno della Struttura, ma anche possibilmente all'interno di aree vaste, di regioni, o addirittura a livello nazionale: si pensi a tutte le iniziative di telemedicina, di comunicazione e di messa in condivisione delle informazioni e dei documenti sanitari oggi in essere. Come si potrebbe strutturare un reperimento e una pubblicazione dei documenti, senza una fondata garanzia di reperimento sicuro e veloce degli stessi? Ad esempio, la corretta classificazione di un referto, di un'immagine radiologica, dell'esito di un'analisi di Laboratorio, sulla

cui conservazione esistono tempi certi ed imposti dalla legge, è uno degli elementi di garanzia che concorrono a dare certezza sull'autenticità di un documento.

Dopo una rigida impostazione iniziale, è necessario avviare anche un attento controllo su tutto il processo di generazione e gestione della documentazione; la presenza di sistemi di allarme che permettano di prevenire, identificare e correggere le anomalie possono incidere sulla sicurezza e sulla precisione del risultato finale. La responsabilità non sta pertanto solo nella validazione di quest'ultimo, ma anche nella predisposizione, attivazione e miglioramento di un sistema di qualità, nel quale le procedure vengono progettate ed avviate per mantenere la migliore gestione possibile in tutte le fasi, soprattutto per permetter l'indispensabile utilizzo clinico delle informazioni prodotte.
Una volta creato il documento con gli elementi archivistici necessari nel contesto di appartenenza, esso va arricchito continuamente con le informazioni di contesto, fino a giungere alla conservazione permanente. Così si riesce a garantire il governo e la corretta custodia del documento nella continuità dei passaggi di vita di esso, con tracciatura delle operazioni e delle responsabilità legate, che gli archivisti chiamano 'traditio' della fonte o 'storia archivistica'.
Per meglio comprendere i concetti teorici sopra esposti, si porta un esempio in ambito radiologico: quando le evidenze informatiche vengono trasferite sul sistema PACS (Picture Archiving and Communication System), ove vengono sottoposte ad archiviazione con l'apposizione di un riferimento univoco, secondo le modalità implementate nell'apparecchiatura. La scelta di un tale riferimento univoco deve essere impostata in maniera da ricondurre in modo esclusivo al paziente sul quale l'esame è stato eseguito e per il quale le immagini sono state prodotte, ad uno specifico contesto clinico, a quella determinata richiesta di prestazione e ad un solo referto al quale l'immagine radiologica sarà indissolubilmente legata da una corretta classificazione.

Ove ciò non sia stato così impostato sino ad oggi, le Strutture che ritengono di voler migrare verso la gestione di un intero ciclo documentale digitale a pieno valore legale dovranno provvedere anche ad una preliminare riorganizzazione nei seguenti ambiti: individuazione delle aree organizzative omogenee, istituzione di un unico protocollo generale, istituzione del Servizio archivistico e individuazione formale del suo responsabile. Risulta inoltre necessario riorganizzare i flussi documentali, legandoli al censimento dei procedimenti amministrativi, oltre che individuare i responsabili dei singoli procedimenti, predisporre e introdurre l'uso di un 'titolario' di classificazione dei documenti, che consenta di garantirne l'univoca identificazione nel tempo, attraverso una corretta protocollazione, classificazione e fascicolazione dei documenti stessi.

All'Amministrazione archivistica del Ministero per i beni e le attività culturali sono conferiti (dal D.lgs n.42/2004, art. 10 e dal regolamento di organizzazione del Ministero per i beni e le attività culturali) i poteri di vigilanza e controllo sugli archivi pubblici, oltre che le funzioni a sostegno delle Pubbliche Amministrazioni nella fase di progettazione e creazione del proprio sistema archivistico. Ciò ha lo

scopo di assicurare la corretta conservazione dei documenti nel tempo, predisponendo anche modelli di Titolario di classificazione, Prontuario di scarto, Regolamento d'archivio e Manuale di gestione, specificamente destinati alle Aziende sanitarie locali, già oggi utilizzati in diverse Strutture Sanitarie.

2.7.2. *Scarto*

E' corretto a questo punto ricordare che esiste anche una procedura cosiddetta di 'scarto' della documentazione appartenente agli archivi degli Enti pubblici, prevista dalla normativa vigente (Codice dei beni culturali e del paesaggio, D.lgs 22 gennaio 2004, n.42, art.21) come operazione soggetta all'autorizzazione della Sovrintendenza archivistica competente per territorio.

In linea generale, la norma asserisce che lo scarto dei documenti d'archivio può essere ammesso quando si verificano le condizioni dell'esaurimento dell'utilità giuridico-amministrativa dei documenti e della mancanza di apprezzabile interesse come fonte storica degli stessi e del loro contenuto.

Per porre in essere la selezione e l'invio alla distruzione dei documenti, nei singoli settori della Pubblica Amministrazione vengono approntati, in accordo con l'Amministrazione archivistica, gli elenchi (cosiddetti 'massimari' di conservazione e scarto) dei vari tipi di documento tipici, come per esempio il "Prontuario di scarto per le Aziende Sanitarie" locali (http://www.archivi.beniculturali.it/divisione_III/schola_salernitana.html).

Seguendo le procedure predisposte dalla normativa vigente, ogni richiesta di avviare lo scarto deve esser adeguatamente motivata con indicazione, per ogni serie, del motivo per il quale si ritiene sia venuto meno l'interesse giuridico-amministrativo e perché non si ravvisi la necessità di una conservazione per scopi storici.

Oggetto di scarto non sono i singoli documenti ma le loro aggregazioni (serie tipologicamente omogenee oppure fascicoli disomogenei al loro interno, ma uniformi per le modalità della loro formazione). Quindi, è consigliabile che l'organizzazione dell'archivio corrente tenga conto della futura necessità di conservare solo parte della documentazione prodotta; pertanto è il caso di prevedere, ad esempio, la creazione di sottofascicoli facilmente individuabili ed estraibili al momento dello scarto, mentre si può avviare la conservazione della parte fondamentale del fascicolo medesimo.

La procedura di scarto, per l'archivio di un ente pubblico, si svolge in quattro fasi:

1. Il dirigente dell'Ente trasmette alla Soprintendenza archivistica, con lettera protocollata, l'elenco in due copie, entrambe da lui firmate, delle tipologie archivistiche che si ritiene non abbiano più utilità amministrativa.
2. La Soprintendenza archivistica restituisce una copia dell'elenco, vistato con approvazione totale o parziale.
3. Nel caso di documentazione cartacea, l'Ente provvede a cedere i documenti da scartare alla Croce Rossa Italiana, o, in caso di indisponibilità della medesima, a organizzazioni, anche di volontariato (ex DPR 8/1/2001 n.37, art. 8), che ne garantiscano la distruzione (tramite triturazione, incenerimento,

macerazione a fine di riciclare il materiale).

4 Infine l'Ente trasmette alla Soprintendenza archivistica copia del verbale attestante le modalità dell'avvenuta distruzione.

E' perciò legittima e normativamente prevista la possibilità di scartare i documenti quando sia riconosciuto l'esaurimento dell'utilità giuridico-amministrativa di essi e la mancanza di apprezzabile interesse come fonte storica degli stessi e del loro contenuto. Ma ormai tutti concordano che lo scarto dei documenti nativamente analogici, trasformati in digitali, non debbano essere sottoposti alla distruzione, ma debbano essere mantenuti su supporto analogico per i tempi imposti dalle norme specifiche a cui ognuno di essi si deve riferire. In ambito clinico-sanitario, invero, si continua a ritenere che le informazioni raccolte non vadano mai a perdere interesse e, anche se i documenti che le contengono possono essere trasformati in documenti informatici, non vi sono controlli sufficienti affinché il procedimento di trasformazione venga posto in essere tecnologicamente e funzionalmente nel migliore dei modi.

Conseguentemente, se la gestione di un nativo documento informatico viene vista positivamente ormai da tutti, perché assicurata nell'intero ciclo di vita da tecnicismi e norme, la trasposizione dall'analogico all'informatico è ancora oggi guardata con occhio del tutto critico ed ovunque rifiutata per mancanza di sicurezze anche medico-legali.

2.8. PROTOCOLLAZIONE

Nell'attuale visione amministrativa che la normativa rispecchia, i sistemi di protocollo informatico e di gestione documentale hanno il compito di diventare gli arnesi indispensabili a mettere in atto i programmi di trasparenza studiati per i rapporti fra amministrazioni e fra amministrazioni e cittadini.
La protocollazione esprime una fase importante nella gestione dei sistemi documentali nella Pubblica Amministrazione. Il protocollo è uno strumento necessario durante la fase di formazione e strutturazione di un archivio, al fine di regolare le fasi di produzione e gestione della documentazione. A prova di ciò, si ricordi che il Legislatore, già prima nel DPR n.428/98 e poi nel DPR n.445/00, ha disposto per la PA l'obbligo di adottare sistemi di protocollo informatico e di gestione documentale. Quindi, essendo stato riconosciuto il protocollo come il fulcro dei flussi di lavoro nella PA, questa sarebbe costretta ad affrontare la ridefinizione dei flussi documentali, e conseguentemente, l'introduzione o l'aggiornamento dei sistemi di classificazione, la strutturazione dell'archivio quale elemento fondamentale della Struttura.
L'introduzione normativa del concetto di documento informatico e del suo ciclo di vita è stata sostanziale per giungere all'informatizzazione del protocollo, dell'utilizzo delle firme elettroniche e l'attivazione dei sistemi di conservazione nel tempo dei documenti digitali.

E' ritenuto che una registrazione di protocollo, quale memorizzazione delle informazioni relative al documento nel registro di protocollo, debba corrispondere all'assunzione di responsabilità da parte dell'ente, nonché alla certificazione dell'esistenza del documento a partire da un certo momento temporale. L'amministrazione stessa può impiegare lo strumento della protocollazione informatica a fini probatori, allo scopo di dimostrare, ad esempio, che un documento sia stato prodotto e che a decorrere da una certa data sia in grado di produrre i suoi effetti.
Indispensabile, dopo la fase di protocollazione, che si provveda, come più sopra affermato, all'adozione di un titolario che permetta all'Ente di archiviare i documenti protocollati seguendo i principi di classificazione predeterminati, permettendo così di svolgere agevolmente la ricerca dei documenti.
La normativa pone i principi generali e specifica i requisiti del sistema, inoltre stabilisce quali sono le regole organizzative interne e le caratteristiche che devono possedere i sistemi tecnologici che ogni ente è tenuto ad adottare per essere in grado di fornire i servizi di certificazione e di gestione dei documenti. Ciò tenendo conto delle necessità di sicurezza e integrità dei dati, e garantendo solo gli accessi autorizzati e legittimati, in ottemperanza con la normativa sul data protection nel trattamento dei dati personali. Per questi motivi la Pubblica Amministrazione è obbligata dalla legge ad individuare al proprio interno un insieme di "Aree Organizzative Omogenee" (AOO). Ciascuna AOO deve essere dotata di un sistema di protocollo informatico che realizzi alcune funzionalità di base (nucleo minimo), deve mantenere un registro informatico, deve istituire un servizio con un responsabile, deve assicurare che venga eseguita la protocollazione dei documenti scambiati con soggetti esterni all'ente.

Ecco come si dimostra facilmente che un sistema di protocollo informatico costituisce la prima base per l'avvio dell'automazione dei procedimenti della Pubblica Amministrazione, o come minimo per il supporto all'informatizzazione dei workflow.

2.9. POSTA ELETTRONICA CERTIFICATA (PEC)

L'e-mail è lo strumento di trasmissione elettronica dall'enorme valenza culturale, sociale e comunicativa, da utilizzarsi per l'invio di messaggi e documentazione, all'interno della PA, fra questa ed i privati e fra i privati.
La Posta Elettronica Certificata (PEC) era stata prevista e disciplinata nel DPR 11 febbraio 2005, n. 68, con l'intento principale di regolamentare un sistema che garantisse i momenti dell'invio e della ricezione dei messaggi di posta elettronica, rendendo la trasmissione stessa del messaggio, la data e l'ora di trasmissione o di ricezione e il mittente opponibili ai terzi. Infatti, l'art.4 del DPR n.68/05 asserisce che "la posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge". Tale obiettivo è raggiunto mediante la previsione di un sistema di "tracciatura" del percorso effettuato dal messaggio di posta elettronica.
I punti salienti del provvedimento normativo concernente la PEC sono qui di seguito schematizzati:

- Il CNIPA ha predisposto e, allo stesso tempo, mantiene un apposito elenco dei cosiddetti Gestori del servizio (art.14 del DPR n.68/05), verificandone i requisiti soggettivi ed oggettivi (capacità ed esperienza tecnico-organizzativa, gestione della sicurezza, certificazione del processo,...). I Gestori vanno considerati i "garanti" dell'avvenuta consegna;
- I messaggi devono essere sottoscritti con la firma digitale del Gestore, al fine di garantire l'integrità e l'autenticità del messaggio;
- I Gestori sono obbligati a verificare la presenza di virus nei messaggi e-mail e comunicare quindi il mittente tali anomalie, bloccando la trasmissione (art.12);
- Le imprese possono esplicitamente dichiarare la propria disponibilità-volontà a ricevere PEC, all'atto dell'iscrizione al registro delle imprese.

Il DPR n.68/05 impone alcune regole di sicurezza da ottemperare nel tragitto telematico della e-mail. Secondo l'art.11 i Gestori devono mantenere traccia di tutte le operazioni eseguite, attraverso un registro informatico ad hoc e per un tempo prestabilito. E' importate che i medesimi Gestori si organizzino con servizi di emergenza atti a garantire il compimento delle trasmissioni ed il rilascio delle ricevute. Tutte le tracce informatiche così conservate hanno lo stesso valore giuridico delle ricevute e sono probatoriamente opponibili ai terzi.

Su alcune osservazioni inerenti agli aspetti giuridici e funzionali del sistema di PEC vale la pena soffermarsi:

1) Certezza e sicurezza della trasmissione

L'art.6 del DPR n.68/05 afferma che quando il mittente invia il messaggio di posta ottiene dal proprio Gestore una ricevuta, ossia un messaggio attestante l'avvenuta spedizione. Questa ricevuta, chiamata "*di accettazione*", dovrà contenere i dati di certificazione: i dati riguardanti la trasmissione del messaggio di PEC, comprendenti anche i riferimenti temporali necessari. Nel sistema sono previste anche altre ricevute, aventi lo stesso meccanismo e lo stesso compito. La ricevuta "*di avvenuta consegna*" procura al mittente la prova che il suo messaggio di PEC è giunto all'indirizzo e-mail dichiarato dal destinatario; ciò peraltro indipendentemente dalla sua effettiva avvenuta lettura. La ricevuta "*di mancata consegna*" concerne, invece, il caso in cui il messaggio di posta non risulti consegnabile al destinatario. Il DPR prevede espressamente all'art.8 che questa ricevuta debba essere recapitata al mittente entro ventiquattro ore dall'invio.

Il DPR ha voluto dare forte rilevanza legale alle fasi dell'invio e della consegna del messaggio, prevedendo due importanti e distinte presunzioni, di invio e di consegna, che si formano nel momento in cui il messaggio viene inviato e quando il messaggio stesso appare essere disponibile presso l'indirizzo del destinatario.

2) Valore ed efficacia probatori della trasmissione del messaggio

E' importante premettere che il sistema di PEC non si interessa minimamente della rilevanza del contenuto del messaggio. Il DPR non è rivolto a garantire l'integrità e la provenienza del messaggio in sé, invece esso si limita a garantire il valore giuridico dell'invio e della ricezione, ovvero i due momenti centrali della trasmissione della e-mail.
Il DPR sostiene che il messaggio di PEC è un documento informatico, ma non affronta la rilevanza giuridica e l'efficacia probatoria del messaggio in sé. Riconosce una particolare rilevanza giuridica alla trasmissione dei messaggi oggetto della procedura che si sta qui approfondendo, utilizzando la firma elettronica qualificata come strumento che permette un tale esito. L'art.9 del DPR n.68/05 prevede che il Gestore di posta elettronica certificata debba sottoscrivere con firma elettronica qualificata le ricevute rilasciate, al fine di verificare la provenienza e l'integrità delle ricevute, permettendo inoltre la certificazione di data e ora di invio e ricezione del messaggio con opponibilità ai terzi. Secondo certa Dottrina, perché fosse garantita l'integrità e la provenienza del messaggio, sarebbe stato opportuno che fosse prevista direttamente la validazione del messaggio stesso con firma elettronica qualificata da parte del mittente. Quindi poteva essere preferibile non la firma della ricevuta, ma del messaggio; firma eseguita non da parte di un soggetto terzo, ma del mittente del messaggio.

3) Il Gestore del servizio di posta elettronica certificata

Il Gestore di PEC - il quale ha il controllo del sistema e ne è responsabile - è il soggetto, pubblico o privato, che svolge le funzioni sopra descritte solo se iscritto nelle liste apposite tenute dal CNIPA, il quale ultimo deve attuare tutte le attività di vigilanza e controllo. Ogni utente è libero di scegliere il Gestore che preferisce, comportando ciò la possibilità che mittente e destinatario del messaggio si servano quindi di Gestori diversi, che devono comunque garantire la standardizzazione e l'interoperabilità tra le attività e i trasferimenti che svolgono. Per questo peculiare motivo, l'art.7 del DPR n.68/05 contempla l'esistenza di un'ulteriore ricevuta, riguardante la presa in carico e che viene rilasciata dal Gestore del destinatario a quello del mittente, nel momento in cui il messaggio viene appunto preso in carico. L'interoperabilità è elemento essenziale e imprescindibile per permettere il colloquio fra i privati, ma soprattutto fra questi e la Pubblica Amministrazione.

2.10. TEMPO INFORMATICO

Come ormai più e più volte qui affermato, ancor prima di progettare una gestione di documenti clinico-sanitari, è fondamentale prendere in considerazione ed implementare, a seconda delle necessità di scenario, ogni misura atta a garantire la correttezza ed il controllo dei processi e delle procedure, contemplati dalla normativa vigente anche in tema di sicurezza e di riservatezza nel trattamento dei dati.
Una di queste indispensabili misure è rappresentata dalla gestione sicura della sincronizzazione degli orologi di tutti i sistemi informatici ed informativi coinvolti nella gestione informatizzata dei documenti, al

fine di determinare con precisione la sequenza temporale di ogni azione e, conseguentemente, l'intervento di ogni soggetto fisico o device.
Onde applicare il tempo (in modo 'certo' o anche solo 'vero') alle azioni, ai messaggi o ai documenti, il Legislatore ci ha messo a disposizione vari strumenti informatici, da utilizzarsi a seconda delle esigenze del contesto: evidenza temporale, riferimento temporale e validazione temporale. A seconda delle caratteristiche dei sistemi e dei bisogni per i quali viene utilizzato, per l'applicazione del tempo ci si deve basare sui principi informatici che stanno a fondamento delle tipologie ora riportate.
Quindi, anche se per determinate attività o documenti non viene prevista da norme o codici l'identificazione del momento temporale per la loro esistenza giuridica, da un punto di vista specifico clinico, amministrativo e medico-legale risulta essere obbligatoria. Quindi, la fedele sequenzialità degli eventi può divenire più che mai necessaria anche se si vogliono soddisfare un giorno pretese probatorie. In altre parole, vanno adottate delle soluzioni che permettano di gestire il tempo sia degli eventi sia dei documenti. Invero, in ambito clinico-sanitario e amministrativo vengono trattati dati e documenti che contengono, e devono contenere, informazioni temporali che non ricadono necessariamente nella problematica della validazione temporale (come per esempio la marca temporale). E tali informazioni, come si capirà meglio più avanti, è utile che vengano inserite nei vari documenti da firmare e/o conservare (ad esempio, l'ora di esecuzione di un esame radiologico dovrebbe essere congruentemente corrispondente sia nel referto sia nelle immagini).

Normativamente vengono individuate due tipologie di tempo informatico, con caratteristiche tecnologiche, funzionali e probatorie differenti. A seconda delle esigenze operative e degli scenari, gli utilizzatori potranno scegliere fra:

- il *riferimento temporale*, che già il DPCM 13.1.04, all'art.1, co.1, lett.g) definiva come la "informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici"
- la *validazione temporale* che il DPCM 13.1.04, all'art.1, co.1, lett.h) definiva come "il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi".

2.10.1. *Riferimento temporale*

Si deve preliminarmente ricordare che, per la validità giuridica della scrittura privata e della rappresentazione meccanica, il Legislatore non ha previsto quali elementi essenziali la data e l'ora di composizione e di firma del documento. Data e ora divengono essenziali, invece, nel caso si voglia redigere un atto pubblico, nel quale esse debbono rivestire la caratteristica della certezza. Il momento temporale è ritenuto invece come necessario per la scrittura privata e la rappresentazione meccanica se si vogliono soddisfare pretese probatorie. Si può assicurare come non vi sia imposizione normativa o

necessità di associare un tempo alla firma di certi documenti, in modo da poter definire con certezza il momento in cui esso è stato firmato. E' chiaro, come già evidenziato, che questa mancanza cozza con le esigenze proprie dei sistemi informativi che gestiscono per esempio i documenti clinico-diagnostici (referti, cartelle, immagini, etc.), dove invece la fedele sequenzialità degli eventi è sentita come principio fondamentale. Basti pensare ad un ipotetico caso assurdo dove, a causa di un disallineamento degli orologi dei sistemi, le immagini radiologiche abbiano un momento temporale successivo a quello del referto.
Da queste poche osservazioni si comprende bene che non per tutto ciò che necessita operativamente di una datazione, può essere utilizzata una validazione temporale: la norma parla, infatti, di essa come apponibile "ad uno o più documenti informatici". Ma non tutte le informazioni importanti vengono tradotte in documento informatico. Quindi vanno rinvenuti meccanismi tecnologici rispondenti alla necessità di una datazione sicura anche a dati e ad attività che non siano solo documenti.

2.10.1.1. Consistent Time

Per superare le criticità qui sopra esposte, una soluzione di riferimento temporale quanto mai rispondente è stata rinvenuta nell'apposito profilo di integrazione proposto da IHE, ovvero il Consistent Time (CT), descritto nel Technical Framework del dominio ITI. La semplice soluzione, basata sul protocollo "network time" largamente utilizzato, permette di allineare in modo preciso gli orologi di tutti i sistemi informativi sanitari coinvolti. Il beneficio di adottare questa soluzione per la dematerializzazione è quello di poter essere ragionevolmente garantiti che le informazioni temporali inserite in modo automatico all'interno dei sistemi, e poi anche dei documenti generati dai sistemi stessi, siano coerenti con il flusso processuale.
E' più che evidente che il Consistent Time non sia un elemento o un sistema previsto dalla norma ai fini della dematerializzazione della documentazione clinico-sanitaria; esso risulta peraltro essere anche una valida misura di sicurezza adottabile nel trattamento delle informazioni. Il tempo così ottenuto non viene previsto dalla norma come un elemento di prova 'opponibile ai terzi', poiché riferimento temporale e non validazione, e deve essere invece classificato come una prova semplice. Va a questo punto evidenziato come la non opponibilità ai terzi non significhi che il tempo così ottenuto, da un punto di vista probatorio, non valga nulla. Varrà, infatti, come presunzione semplice, che è comunque una prova e come tale potrà essere discrezionalmente utilizzata e riconosciuta dal giudice a supporto di una sua decisione.

2.10.1.2. Signing Time

Una metodologia per aumentare la sicurezza nell'utilizzo del sistema di firma digitale e per rispondere ancora alle esigenze di applicazione di un tempo sicuro, è quella dell'utilizzo del *signing time*. In modo completamente automatico e non modificabile dall'utente, all'atto dell'apposizione della

sottoscrizione si può inserire un attributo interno alla stessa firma digitale, contenente la data e l'ora in cui essa viene apposta. In questo modo si è in grado di legare strenuamente il documento da firmare al dato temporale, garantendolo proprio con la stessa firma digitale da possibili successive alterazioni. Tale attributo è previsto nella stessa firma digitale, e la sua apposizione è sincrona al processo di sottoscrizione, ovvero si riferisce in modo indissolubile ad essa. Si tratta di un forte elemento per l'aumento della sicurezza del sistema, ma esso riguarda solo la firma digitale del documento e non tutte le altre attività, e inoltre, come per il Consistent Time, non vi è imposizione normativa alcuna che ne contempli l'utilizzo.

2.10.2. *Validazione temporale*

La norma prevede di poter applicare al documento alternativamente ben quattro tipi di riferimento temporale che, a differenza di quelli descritti nei paragrafi precedenti, possa essere considerato una prova opponibile ai terzi. L'art.1, co.1, lett. bb) del D.lgs n.82/05 ribadisce il concetto dalla normativa precedente già impostato, secondo il quale la validazione temporale è "il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi".

Inoltre l'art.39 del DPCM 13.1.04 prevede fra le validazioni temporali, oltre alla marca temporale, altri tre sistemi opponibili ai terzi: "a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272; b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti; c) il riferimento temporale ottenuto attraverso l'utilizzo di posta certificata ai sensi dell'art. 14 del testo unico".

Le quattro modalità di validazione temporale possono essere alternativamente utilizzate, ma nella pratica, a seconda dell'ambiente in cui ci si trova, dovranno essere scelti i sistemi più calzanti alle esigenze dello scenario. Invero, a titolo di esempio, la segnatura di protocollo e la posta elettronica certificata risulterebbero di difficile applicazione pratica al mondo clinico, mentre potrebbero essere largamente apprezzati ed utilizzati in ambiente amministrativo.

La conservazione sostitutiva merita una piccola considerazione in più: si può affermare che, per la tipologia di documenti in genere trattati in ambito clinico-sanitario, vi sia molto spesso l'obbligo normativo di sottoporli sempre e comunque a tale procedimento di validazione temporale. Tuttavia il tempo che intercorre fra la firma del documento e l'avvio del processo di conservazione potrebbe essere ritenuto troppo lungo e quindi far propendere per un ulteriore livello di sicurezza, introducendo nel flusso anche l'elemento della marca temporale.

Comunque va evidenziato che tutti i procedimenti di validazione temporale, oltre ad essere utilizzabili solo su un documento e non per attività o messaggi, sono anche tipicamente asincroni rispetto a quelli della creazione, della sottoscrizione, dell'archiviazione o della comunicazione del documento: sono

utilizzabili solo in un momento diverso, e sicuramente successivo, da quello in cui vengono poste in essere tutte le operazioni tecnologiche e funzionali necessarie. La validazione temporale è quindi, per esempio, in grado di dare la certezza che il documento già firmato esista (dal punto di vista probatorio con riconoscimento di opponibilità ai terzi) a partire dal momento in cui essa venga applicata al documento; ma non esclude, anzi, che il documento sia esistito precedentemente, fino a prova contraria. La validazione temporale mediante apposizione di marca temporale ad un documento informatico equivale quindi alla determinazione della 'data certa', che nel nostro ordinamento si può ottenere per la documentazione analogica nei previsti seguenti modi: con la morte del soggetto, con l'accertamento giudiziale, con la sottoposizione dello scritto alla formalità di registrazione presso l'Ufficio del Registro, con la vidimazione presso notaio o altro ufficio pubblico.

2.10.3. *Verifica del potere di firma*

Come meglio accertabile nei paragrafi dedicati alle firme e ai certificati di firma, un punto assai delicato per tutta la sicurezza del sistema di dematerializzazione/gestione documentale interamente digitale è la verifica della validità del certificato di firma e il conseguente posizionamento nel tempo del documento firmato. Ovvero, si parla della situazione in cui un certificato di firma risulti scaduto, revocato o sospeso ed il documento firmato non temporalmente collocabile, al fine di poter provare che era stato firmato prima della scadenza/sospensione/revoca del certificato.

L'art.21 del D.lgs n.82/05 afferma che "3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata 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". Rimane affidato alla libera valutazione del Giudice il riconoscimento della rispondenza di un tale documento al requisito della forma scritta (art. 20, co. 1 bis, D.lgs n. 82/05) e se utilizzarlo ugualmente a scopi probatori. Ancora al Giudice viene riconosciuta comunque la facoltà di accertare, anche attraverso altri mezzi di prova, la conformità dei fatti e delle cose rappresentate nel documento.

Onde evitare un simile e grave problema di gestione della validità dei documenti firmati digitalmente, una soluzione potrebbe essere sicuramente quella di apporre un riferimento temporale al documento firmato, nei modi più sopra descritti. Ma al fine di evitare sin da subito l'eventualità di dover gestire a posteriori la valenza giuridica, probatoria e quindi anche clinica di un documento sottoscritto con firma avente certificato scaduto/revocato/sospeso, vi è la possibilità di verificare la validità del certificato al momento dell'apposizione della firma stessa. Poiché imposto dalla normativa vigente sulla data protection, sarebbe buona regola che gli applicativi di creazione e gestione del documento verificassero sempre, mediante il controllo degli accessi, le credenziali dell'utente, in modo da poter verificare immediatamente se egli è

abilitato ad entrare nel sistema, ma anche a sottoscrivere. Se a questa procedura legata alla sicurezza e alla riservatezza nel trattamento dei dati, si aggiungesse anche la verifica della validità del certificato di firma, allora si sarebbe in grado di stabile con certezza non solo che il soggetto aveva le credenziali per poter firmare, ma anche che il suo certificato di firma era valido al momento della firma stessa: ecco il cosiddetto potere di firma. Questa procedura, sentita più come una misura di sicurezza, risulta anche di fondamentale importanza per risolvere altri problemi, comunque correlati al trattamento delle informazioni, poiché, unitamente all'apposizione del riferimento temporale apposto sul documento, si otterrebbe la sicurezza a priori che il documento stesso, redatto e firmato sia, dal punto di vista clinico nei tempi, da un punto di vista legale e medico-legale nella validità, un documento che possiamo tranquillamente distribuire ai soggetti interessati.

3. CONSERVAZIONE

Negli ultimi anni, la continua evoluzione tecnologica ha portato all'emanazione di tante norme, con la volontà di soddisfare le esigenze generali dell'informatizzazione. Ma al rinnovamento tecnologico continuo non sembrano corrispondere i desideri del mondo pratico, forse anche a causa dei retaggi culturali propri di ogni ambito, consuetudinari e legati al vetusto supporto analogico, al quale vengono ancora ampiamente riconosciute le proprietà di inalterabilità e di autenticità volute.

Ci si può ben rendere conto che le logiche e le prassi connesse alla funzione conservativa della documentazione digitale conducono ad una notevole trasformazione di quelle proprie del mantenimento nel tempo dei documenti analogici (su carta, pellicola, filmato, etc.). Come ogni modernizzazione, anche il processo di conservazione necessita di seri approfondimenti in ogni settore da parte di tutte le competenze: risulta essere un grosso errore il lasciare che la diversificazione selvaggia di implementazioni ostacoli l'armonizzazione, che l'obsolescenza dei supporti non consenta di avviare organici piani di utilizzo protratti a lungo nel tempo (così come invece impone molta parte della normativa in ambito clinico-sanitario).

Conseguentemente il Legislatore ha tentato di porre le basi per individuare metodi e procedure implementative condivisi, oltre che standard e regolamentazioni adeguati, applicabili a seconda degli ambienti da trattare.

La conservazione digitale, dopo la produzione del documento, rappresenta il passaggio essenziale per giungere all'insieme delle attività che permettano la persistenza nel tempo in un ambiente tecnologico dell'accessibilità, della leggibilità, della intelligibilità, dell'autenticità, della integrità del documento digitale. Il processo normativo ha quindi tenuto conto di questa complessa trasformazione, emanando una serie di provvedimenti di portata generale, applicabili orizzontalmente. Per i settori più avanzati della Pubblica Amministrazione si è inoltre sentita l'esigenza di esemplificare e armonizzare e i contenuti normativi alle peculiarità funzionali.

3.1. BANCA DATI, ARCHIVIAZIONE E CONSERVAZIONE

Questo passaggio viene talvolta poco approfondito nei sistemi di dematerializzazione, soprattutto nei suoi significati sostanziali e anche perché non obbligatorio per la norma. Appare pertanto utile ricordare alcune astratte definizioni e qui interpretarle e calarle nell'ambito sanitario che ci interessa. La norma (Deliberazione CNIPA n.11/04, art.1, co.1, lett.f) definisce *memorizzazione* "il processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti". Nei sistemi RIS e LIS questo è da vedersi come il procedimento di salvataggio del referto firmato. Altresì, la medesima Deliberazione definisce l'*archiviazione elettronica* come "il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione".
Da qui parrebbe che l'unica differenza fosse legata al codice univoco, ma, in effetti, si può individuare qualche cosa di più: per conservare analogicamente o elettronicamente i documenti bisogna che essi siano sottoposti prima al processo di classificazione e fascicolazione. Così come ampiamente dimostrato più sopra, l'attività di classificazione appare essere molto delicata, perché prevede di entrare nel merito del documento, con verifica della presenza al suo interno degli elementi ritenuti necessari, quali per esempio il nome del paziente, l'identificativo univoco del paziente, etc. Se pensiamo ad uno scenario, normativamente plausibile, in cui tutta la conservazione ottica dei documenti venga effettuata all'esterno della Struttura Sanitaria, risulta difficile ipotizzare che l'attività preliminare di questo procedimento sia anche lo svolgimento della verifica degli elementi previsti dalla classificazione. Risulta quindi una buona regola di sicurezza l'inserimento di un sistema di archiviazione, interposto fra la memorizzazione (come per esempio i sistemi RIS o LIS nell'ambito clinico) ed il sistema di conservazione, al fine di supportare correttamente proprio le funzionalità della classificazione.

In qualsiasi Struttura la banca dati, sia essa clinica o amministrativa viene predisposta ed organizzata esclusivamente con il fine dell'utilizzo corrente del documento: se questo ad esempio è clinico, lo scopo della banca dati è quella di poter consultare la documentazione precedente e quindi ricostruire il quadro clinico del paziente per migliori diagnosi, cura ed assistenza. Le regole per la tenuta di una tale banca dati non vengono individuate da norma alcuna; la strutturazione e la gestione possono pertanto essere attuate su libera iniziativa e con modalità scelte dagli implementatori e dagli utilizzatori.
L'archivio legale è invece espressamente previsto da disposizioni normative che ne individuano i contenuti, e ne dettano le specifiche modalità per la formazione e la gestione: gli scopi della sua esistenza sono quindi quelli prettamente amministrativi, medico-legali e probatori.
E' stata totalmente attuata l'equiparazione giuridica fra l'archivio legale analogico e quello digitale, sempre che siano soddisfatte per entrambi le regole di gestione prescritte dalle norme. La Deliberazione CNIPA n. 11/04 all'art. 2, co.1 asserisce, invero, che "Gli obblighi di conservazione sostitutiva dei documenti previsti dalla legislazione vigente sia per le pubbliche amministrazioni sia per i privati, sono

soddisfatti a tutti gli effetti ... qualora il processo di conservazione venga effettuato con le modalità di cui agli articoli 3 e 4". Il D.lgs n.82/05, co.1 sancisce addirittura che le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici". L'art.43 del medesimo Decreto afferma anche che "1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo. ... 2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali. 3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali".

Dai contenuti del Codice dell'Amministrazione Digitale quindi si evince che un documento informatico, per il quale vi sia normativa che obblighi il suo mantenimento nel tempo per scopi legali e probatori, deve assolutamente essere sottoposto a conservazione, anche se il suo trattamento intermedio fra creazione e conservazione può sempre avvenire su supporti analogici (carta, pellicola, etc.), per rispondere alle esigenze organizzativo-funzionali dello specifico settore in cui si opera.

3.2. IL RESPONSABILE DELLA CONSERVAZIONE

Negli ultimi tempi si rinvengono differenti impostazioni dottrinali in merito ad alcuni aspetti legati alla figura del Responsabile della conservazione e alla sua individuazione all'interno o all'esterno della Struttura che produce la documentazione da sottoporre a conservazione. Onde inquadrare il problema e individuare le scelte più congrue per il così particolare ambito clinico-sanitario, si richiameranno qui le norme e anche le interpretazioni sia dei cultori della materia, sia dei Tavoli di approfondimento del CNIPA per attuare un'interpretazione critica dell'argomento e sposare un'impostazione lineare: Deliberazione CNIPA n.11/04, la bozza del Tavolo Tecnico del CNIPA "La figura del Responsabile della conservazione. Il Responsabile della conservazione: proposte per un profilo" e la bozza di "Proposta di regole tecniche in materia di formazione e conservazione di documenti informatici" della Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione.

3.2.1. *Richiami normativi*

L'art.5 della Deliberazione CNIPA n.11/03 al comma 1 elenca le attività che il Responsabile della conservazione deve porre in essere, perché un sistema per il mantenimento nel tempo della documentazione digitale possa essere implementato e accettabilmente governato. Alcune delle attività citate concernono analisi strategiche che il Responsabile deve eseguire prima e durante il processo di conservazione; altre attività manifestano di avere, invece, connotazione puramente tecnologica; altre attività ancora rivelano, invero, prerogative funzionali e organizzative.

"1. Il responsabile del procedimento di conservazione sostitutiva:
a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;

b) archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:

1) descrizione del contenuto dell'insieme dei documenti;
2) estremi identificativi del responsabile della conservazione;
3) estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
4) indicazione delle copie di sicurezza;

c) mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;

d) verifica la corretta funzionalità del sistema e dei programmi in gestione;

e) adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;

f) richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

g) definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;

h) verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti."

Da tutti i compiti enumerati, si capisce che il ruolo del Responsabile deve possedere competenze di elevata professionalità e anche assai eterogenee. Il Tavolo Tecnico del CNIPA sul Responsabile sostiene, invero, che egli debba possedere le seguenti capacità e conoscenze:

"*Responsabilità principali*

- garantisce la leggibilità dei documenti conservati nel tempo;
- ove previsto, appone sull'insieme dei documenti il riferimento temporale e la firma digitale;
- nelle Pubbliche Amministrazioni svolge il ruolo di pubblico ufficiale e assicura la qualità e l'appropriatezza dei servizi e dei prodotti;
- valuta l'integrità, la leggibilità e l'identificazione dei documenti;
- *può delegare in tutto o in parte le proprie attività ad altri soggetti interni alla struttura;*
- *può affidare in tutto o in parte il processo di conservazione a soggetti terzi.*

Capacità

• capacità di comprensione dei processi amministrativi;

• gestione e trasferimento di conoscenza;

• capacità progettuali e gestionali.

Conoscenze

- archivistica informatica, con particolare riferimento a:
  - standard di rappresentazione dei documenti (ad esempio, nel caso clinico DICOM, HL7 CDA, ebXML, etc.);
  - strumenti di gestione informatica dei documenti;
  - gestione e conservazione di basi di dati, conoscenza dei sistemi di archiviazione e di ricerca;
- sistemi informativi e modelli organizzativi;
- nozioni di base sulle Architetture di Sistemi Informativi automatizzati;
- monitoraggio dei progetti di automazione e acquisizione di beni e servizi informatici (contrattualistica, capitolati);

- nozioni di base di Diritto amministrativo e contabilità dello Stato;
- nozioni di Diritto dell'informatica e delle normative vigenti anche in materia di tutela della privacy;
- metodologie per la gestione dell'innovazione".

3.3. Previsioni di delega e affidamento del procedimento di conservazione

Da quanto riportato sopra, non può che apparire assai difficoltoso, se non del tutto impossibile, trovare in una sola persona fisica tutte le richieste peculiarità professionali. Il Tavolo Tecnico CNIPA ritiene che si debba quindi "ipotizzare la costituzione di un *Ufficio del responsabile della conservazione* cui afferiscano dipendenti con profili professionali archivistici, informatici e manageriali. ... In molte amministrazioni medio-piccole o in sedi periferiche di grandi amministrazioni sarà impossibile prevedere la costituzione di tali uffici e la presenza di dirigenti funzionari con i requisiti e le competenze previste per il responsabile della conservazione. Sembra, quindi, logico prevedere forme federative o consortili, ..., che prevedano un unico ufficio centrale, un unico archivio fisico e attività distribuite", ovvero "l'insieme delle competenze e responsabilità attribuite ad un ufficio o ad una struttura federata".
La "Proposta di regole tecniche in materia di formazione e conservazione di documenti informatici" della Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione all'art.9 asserisce che "2. Il responsabile del procedimento di conservazione può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate. 3. Qualora il procedimento di conservazione sia affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, questi sono tenuti ad osservare quanto previsto dal presente decreto. 4. Le pubbliche amministrazioni nominano il responsabile della conservazione, scegliendolo tra funzionari interni di adeguato profilo. Il responsabile della conservazione svolge il ruolo di pubblico ufficiale, ..., 5. Il responsabile della conservazione opera d'intesa con il responsabile del servizio per la tenuta del protocollo informatico di cui all'art. 61 del DPR 445/2000".

Ancora secondo il Tavolo Tecnico CNIPA, quando l'ambiente in cui si deve lavorare è una Pubblica Amministrazione, "Il Responsabile della conservazione è un funzionario interno alla Amministrazione produttrice della documentazione da conservare. Può essere un dirigente o un funzionario apicale. Il Responsabile della conservazione può delegare in parte lo svolgimento della propria attività ad uno o più persone, ma non può delegare le responsabilità".

Anche l'art.5 della Deliberazione CNIPA n.11/04 sostiene che "2. Il responsabile del procedimento di conservazione sostitutiva può *delegare*, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni

ad esse delegate". Ma al comma 3 dello stesso articolo la Deliberazione sembra fare un balzo ben oltre affermando che "Il procedimento di conservazione sostitutiva *può essere affidato*, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione". La Deliberazione prevede pertanto la possibilità per il Responsabile della conservazione di delegare le attività pratiche a lui proprie; ma in aggiunta, il CNIPA afferma anche che il processo di conservazione può essere affidato a soggetti estranei alla Struttura produttrice della documentazione.
Nel caso della Pubblica Amministrazione quindi il Responsabile della conservazione deve essere individuato all'interno della PA stessa e la nomina deve rivestire la massima portata dell'atto deliberativo aziendale.
Questo trova giustificazione nel fatto che la figura del Responsabile riveste un'elevata importanza per le particolari capacità professionali che gli sono riconosciute dalla normativa vigente, ma soprattutto perché nella realtà deve essere colui al quale vengono riconosciuti poteri funzionali, decisionali ed economici considerevoli. Nella PA, in genere, c'è la convinzione che il mantenimento nel tempo della documentazione prodotta, previsto e regolato anche da specifiche norme di settore, rivesta un peso importantissimo: storico, giuridico, legale e medico-legale. Inoltre, non può essere un ruolo scorporato ed isolato dal resto della Struttura. Il Responsabile deve far parte di quest'ultima e deve essere messo nelle condizioni di collaborare con altri ruoli e con essi deve intraprendere orientamenti decisionali ed applicativi. Il Tavolo Tecnico CNIPA, proprio questo orientamento spinge, sottolineando che il Responsabile della conservazione deve lavorare a stretto contatto con il responsabile dei sistemi informativi e con il responsabile del Servizio per la tenuta del protocollo informatico. Quindi, il ruolo del soggetto preposto al mantenimento nel tempo dei documenti deve assumere responsabilità pesanti e complesse, che non si devono limitare alla pura tecnologia informatica.
A monte deve essere stata prevista una corretta ed articolata strutturazione del sistema di mantenimento nel tempo a valore legale, che vada però a coinvolgere non solo singole entità produttrici di documenti digitali all'interno della Struttura. La complessità delle attività e la specializzazione richiesta per adeguatamente rispondere ai numerosi obblighi previsti dalla vigente normativa rende poco proponibile la figura di un Responsabile della conservazione onnisciente. Quasi impossibile riuscire a pensare ad un soggetto che riesca ad occuparsi di tutti gli aspetti. Pertanto, come è stato proposto dal Tavolo Tecnico CNIPA, un pool di professionalità potrebbe rispondere nel contempo alle esigenze normative e a quelle pratiche.Di conseguenza si capisce che la previsione normativa di poter *affidare* o *delegare* -in tutto o anche solo in parte- il procedimento di conservazione legale ha tutte le ragioni di esistere anche da un punto di vista pratico. Dagli studiosi di questa spinosa materia, si sostiene fermamente che l'affidamento si attua fra la Pubblica Amministrazione e dei soggetti terzi esterni ad essa; mentre l'istituto della delega si effettua in toto nella Struttura, con trasferimento di attività dal Responsabile della conservazione ad altri soggetti, ma sempre interni alla Struttura produttrice della documentazione. Poiché sia nello scenario della delega sia in quello dell'affidamento vengono in gioco profili/livelli di responsabilità con connotazioni sia civilistiche sia penalistiche, e si manifesta forte l'esigenza di verificare con puntualità quali effetti

possano provocare, nei confronti dei vari protagonisti dell'iter procedurale, la divisione dei compiti, l'allocazione delle competenze e le conseguenti assunzioni di responsabilità.

3.3.1. *Affidamento*

Quando si richiama il significato generale di affidamento si pensa alla "esternalizzazione dei servizi", svolti, sino a quel momento, in modo del tutto autonomo all'interno della Struttura. Ma se vi è la crescente consapevolezza di non poter sviluppare oltre al proprio interno le numerose, diversificate e specifiche capacità necessarie ad assicurare la risposta alla modernizzazione, si deve dare in consegna alcune delle proprie attività a qualcuno che sia in grado di svolgerle in modo migliore, contando sulla sua fede, custodia, intelligenza e capacità. Questo è il significato dell'affidamento, secondo la lingua italiana, ma tutto sommato, anche secondo il senso pratico del mondo clinico-sanitario. Con l'esternalizzazione vi è l'affidamento a terzi specialisti dello svolgimento operativo di una o più attività precedentemente svolte all'interno, senza intaccare le prerogative tipiche ed istituzionali del soggetto che se ne avvale.

Tra committente e affidatario si instaura un rapporto, attraverso la stipula di un contratto, che può prevedere vari livelli di coinvolgimento strategico del soggetto scelto. Si realizza così un rapporto basato sul riconoscimento delle reciproche competenze e sulla volontà di dare avvio ad un'effettiva collaborazione professionale, attraverso una tecnica gestionale-organizzativa. Si può così mirare all'innalzamento della qualità dei servizi erogabili, con la semplificazione delle strutture organizzative e burocratiche interne e con l'utilizzo di competenze e tecniche esterne già sperimentate. Esigenze queste che stanno divenendo sempre più sentite anche dalla Pubblica Amministrazione, con una maggiore concentrazione sulle funzioni istituzionali interne.

E' stato ormai dimostrato che la possibilità di affidare a soggetti terzi lo svolgimento di tutto o di parte del procedimento di conservazione legale della documentazione prodotta in PA, così come riconosciuto nella teoria dalla normativa vigente, ha una sua sostanza e una sua percorribilità.

La Corte di Cassazione (sentenza n.21287/2006) ha definito l'esternalizzazione come "il fenomeno che comprende tutte le possibili tecniche mediante cui un'impresa dismette la gestione diretta di alcuni segmenti dell'attività produttiva e dei servizi che sono estranei alle competenze di base (il *core business*)". Quindi, in una Struttura pubblica vengono poste in essere attività cosiddette '*core*' e altre '*no core*'. Le prime rappresentano gli esercizi distintivi dell'organizzazione, fortemente connessi alle finalità istituzionali: nella sanità le attività core sono rappresentate dai fini fondamentali di prevenzione, diagnosi, terapia, cura e assistenza del paziente. Le attività no core qualificano, invece, singoli servizi o specifiche aree di attività di supporto interno, strumentali allo svolgimento delle funzioni principali. Questa tipologia di funzioni mostra possibili aspetti di autonomia e complementarietà, permettendo uno stralcio dal nucleo vitale, attraverso l'affidamento della loro gestione a soggetti esterni all'ente.

Da un punto di vista prettamente giuridico, l'esternalizzazione (chiamata anche outsourcing) viene definita come l'accordo con cui un soggetto (committente) trasferisce ad un altro soggetto (provider, o vendor, o partner) tutte o alcune funzioni atte alla realizzazione degli scopi imprenditoriali. Da qui si comprende che, poiché si tratta di un negozio nato dalla prassi del diritto anglosassone, non riesce ad ottenere una disciplina specifica nell'ordinamento italiano e rientra nei cosiddetti contratti atipici.
L'esternalizzazione può, di fatto, estrinsecarsi in molti modi, così le parti possono regolarla utilizzando sia contratti tipici del diritto italiano sia contratti misti, come il contratto d'appalto, il contratto d'opera, la subfornitura. E' quindi comprensibile che, a seconda delle circostanze, dell'oggetto, delle parti, etc. si creano di volta in volta fattispecie concrete che vadano mano a mano regolate per via contrattuale e che possano produrre rapporti e responsabilità differenti.

3.3.2. *Delega*

Diversamente dalla possibilità di affidare attività a soggetti esterni alla Struttura, la delega deve riguardare il rapporto che si instaura all'interno di essa, ed inoltre con il coinvolgimento di soggetti dell'organizzazione.
La delega è uno strumento giuridico comunemente utilizzato per indicare l'istituto civilistico del "mandato", disciplinato dagli artt. 1703 e 1709 cc.. Il mandato è il contratto con il quale un soggetto si obbliga a compiere uno o più atti giuridici per conto di altri. I due protagonisti del contratto di mandato sono il mandante (che ha necessità di far gestire, tutelare o porre in essere un proprio interesse o specifiche attività) e il mandatario (che abbia la capacità di raggiungere il fine voluto dal mandante e che sia pertanto delegato a compiere gli atti funzionali al perseguimento dell'obiettivo).
Il contratto di mandato è diventato nella prassi quotidiana uno strumento frequentissimo, soprattutto per lo svolgimento delle attività articolate all'interno di organizzazioni e servizi complessi. Ecco perché l'applicazione della delega attraverso il contratto di mandato è richiesta dove vi sia una struttura aziendale avente i caratteri della complessità gestionale, cioè dove le dimensioni e l'eterogeneità della struttura e delle attività portano al bisogno di un trasferimento di mansioni/funzioni, al fine di garantire la reale ottemperanza alle norme. La divisione dei compiti nell'ambito di un'organizzazione complessa trova concreta rilevanza, in quanto la normativa individua una diretta posizione di garanzia in capo a responsabili delle singole unità organizzative (come per esempio nel caso del Responsabile della conservazione ottica sostitutiva).
Si richiama una massima della Corte di Cassazione riguardante la delega nello specifico ambito della tutela infortunistica, che possiede delle similitudini concettuali con gli argomenti che si stanno trattando qui. Cassazione penale del 17/12/97, IV Sez. della (n.286, Pres. Consoli, Ric. Iacono): "L'imprenditore può legittimamente delegare ad altro soggetto gli obblighi su di lui gravanti attinenti alla tutela antinfortunistica solo se si trovi impossibilitato ad esercitare di persona i poteri-doveri connessi alla condizione di naturale destinatario della normativa antinfortunistica, per la complessità ed ampiezza

dell'azienda, per la pluralità di sedi e stabilimenti di impresa o per altre ragionevoli evenienze si da escludere una immotivata dimissione del suo ruolo legale. E' necessario, poi, che il delegante affidi le attribuzioni e le competenze proprie al suo ruolo a persona tecnicamente preparata e capace, che abbia volontariamente accettato la delega nella consapevolezza degli obblighi cui viene a gravarsi, che sia stata fornita dei poteri autorizzativi e decisori autonomi pari a quelli dell'imprenditore e idonei a far fronte alle esigenze connesse all'apprendimento dei presidi antinfortunistici, compreso l'accesso ai mezzi finanziari".

Delega di funzioni e delega di esecuzione

Partendo dai principi esposti dal Tavolo Tecnico interministeriale, secondo i quali nella PA il Responsabile della conservazione deve essere nominato all'interno della Struttura produttrice della documentazione digitale, e che il medesimo soggetto può delegare in tutto o in parte lo svolgimento delle attività sue proprie, l'istituto della delega calza nella fattispecie del nostro Responsabile. A seconda che venga posto in essere un rapporto nascente da *delega di funzioni,* oppure uno scaturente da semplice *delega di esecuzione*, le attività e le relative responsabilità assumono connotazioni differenti.

A) Delega di funzioni

Nelle norme sul riordino della dirigenza statale (L. n.145/02; art.17, co.1 bis, D.lgs n.165/01) è stato riconosciuto ai dirigenti di disporre del potere di delega nei confronti dei dipendenti che ricoprono le posizioni funzionali più elevate nell'ambito degli uffici ad essi affidati e nei quali siano rinvenibili le necessarie professionalità e competenze.
Accertato che la delega va redatta in forma scritta, e quindi in modo certo, si deve evidenziare che:

- essa va conferita a persona professionalmente idonea;
- essa va conferita a persona cui siano attribuiti sufficienti poteri decisionali per poter concretamente attuare le attività previste dalla normativa vigente (es.: Deliberazione CNIPA n.11/04 e Tavolo Tecnico interministeriale "La figura del Responsabile della conservazione. Il Responsabile della conservazione: proposte per un profilo"): il soggetto delegato, oltre a dover possedere le capacità necessarie allo svolgimento delle mansioni, va messo nelle condizioni di svolgere le funzioni a lui assegnate;
- di massima il delegante non deve interessarsi dell'esercizio delle attribuzioni trasferite con la delega.

La *delega di funzioni* sembrerebbe doversi basare sui principi indispensabili delle norme di organizzazione, oltre che sui canoni del diritto civile e di quello penale. Come già accennato, la delega di funzioni si dovrebbe caratterizzare per l'attribuzione di autonomi poteri attuativi e deliberativi al soggetto delegato, il quale deve avere le capacità e le idoneità tecniche sufficienti, senza ingerenze da parte del

delegante. C'è un'assunzione (a titolo derivato) da parte di un soggetto, di una serie di funzioni a lui assegnate da chi ne era in precedenza titolare. La delega di funzioni deve salvaguardare due esigenze di principio: evitare di violare il principio di legalità e di tipicità degli illeciti e quindi, rendere derogabili gli obblighi sanzionati; deve inoltre evitare l'applicazione, in sede giudiziale, di forme oggettive di responsabilità, in capo a soggetti troppo lontani dalla realtà oggetto della fattispecie.
La sentenza n. 39628/04 della Cassazione, ribadisce il principio fondamentale in materia di delega di funzioni, secondo cui, attesa la posizione di garanzia assunta dai vertici dell'ente pubblico, la delega in favore di un soggetto, che per la posizione che ricopre internamente alla Struttura a volte non può neppure rifiutarla (quale è il dirigente o il funzionario preposto), assume valore solo se detti organi siano incolpevolmente estranei alle inadempienze del delegato e non siano stati informati, assumendo un atteggiamento di inerzia e di colpevole tolleranza.

B) Delega di esecuzione

Con la *delega di esecuzione,* il titolare dell'obbligo giuridico affida ad altro soggetto compiti di mera attuazione delle proprie decisioni, peraltro mantenendo pienamente sia la propria posizione di garante sia le responsabilità che da essa ne derivano. Ovvero il titolare assegna ad un terzo l'incombenza di eseguire materialmente alcuni atti, con la realizzazione dei quali al delegato viene trasferita non la competenza ma la legittimazione al compimento di essi, rientranti in realtà nella sfera del delegante. Il delegante non si spoglia della propria posizione, civilmente e penalmente rilevante, e resta il vero obbligato.
Nella delega di esecuzione diviene, pertanto, assai importante il dovere di controllo che deve attuare il delegante sul delegato, durante tutte le realizzazioni oggetto di delega. Ciò poiché il delegante resta il garante principale degli obblighi previsti. Nel momento in cui il delegante ha trasferito ad altro soggetto l'adempimento delle sue attività (con assunzione da parte di quest'ultimo di una posizione di garanzia autonoma ma derivata) assume il rischio dell'inadempimento del delegato e ne risponde, se viene dimostrato che è venuto meno ai suoi doveri di controllo.
Se non vengono poste rigide e chiare linee di demarcazione fra doveri, diritti, oneri e responsabilità derivate, soprattutto in mancanza di accordi contrattuali (delega attraverso contratto di mandato), si rischia che le verifiche dell'inosservanza dei doveri di controllo vengano eseguite solo a posteriori e dal giudice, caso per caso, con riferimento ad una serie di parametri che possono andare dall'organizzazione aziendale, al tipo di delega, ai tipi di soggetti coinvolti, al tipo di contestazione elevata, e così via.
Comunque si ritiene che ai fini della responsabilità penale e civile, il delegante che violi il dovere di controllo deve essere chiamato a rispondere in concorso con il delegato inadempiente. Per esempio, Si ritiene così che i preposti o i soggetti terzi delegati non sono da ritenersi gli unici responsabili dell'inadempimento o dell'incidente derivante dalla mancanza o dall'insufficienza di cautele o mezzi. Per come viene impostata la delega, essi non esplicano un potere di supremazia e di direzione nell'organizzazione della Struttura o su parte di essa.

Va operata ora anche un'ulteriore distinzione all'interno delle possibili responsabilità: capire se il delegante sia esonerato dalla responsabilità oppure rimanga comunque vincolato, sotto il profilo della 'culpa in vigilando'.
Ma prima di affrontare l'interpretazione della fattispecie, è utile riportare i concetti basilari di diritto riguardanti la *culpa in eligendo* e la *culpa in vigilando*. Si ha culpa in eligendo quando il delegato commette un fatto previsto come illecito e si dimostra che non era, sin dall'inizio, in possesso delle condizioni per rendere effettiva la delega. La culpa in eligendo va esclusa quando il delegato assicura la massima idoneità tecnico-professionale e al delegante non si può muovere nessun rimprovero, fino a quando non venga a conoscenza della inosservanza della normativa.
C'è invece culpa in vigilando quando non sia stata verificata la permanenza delle condizioni che avevano portato all'affidamento della delega: il delegante, nel momento in cui ha trasferito ad altri l'adempimento dei suoi doveri, assume il rischio dell'inadempimento del delegato e ne risponde se viene meno ai suoi doveri di controllo, se il contratto e il diritto li abbiano previsti.
Le norme e le interpretazioni dottrinali qui sopra riportati dimostrano che la figura del Responsabile della conservazione dei documenti a pieno valore legale è di fondamentale importanza. Pur rappresentando un ruolo con compiti *no core* della Sanità, il Responsabile della conservazione diviene un importantissimo ruolo di gestione della documentazione che per legge deve essere mantenuta nel tempo, a volte anche illimitatamente.

Per la portata clinica, giuridica e medico-legale molti documenti clinico-sanitari devono essere conservati e, quindi, devono soggiacere ai dettami normativi e alle procedure coinvolgenti in primo piano il Responsabile della conservazione. Ecco perché, per dare risposta alle esigenze di eterogeneità professionali, il Legislatore e il Tavolo Tecnico CNIPA "La figura del Responsabile della conservazione. Il Responsabile della conservazione: proposte per un profilo" hanno pensato sia alla soluzione della creazione di un vero Ufficio interno che operi sulla base dell'istituto della delega, sia alla soluzione dell'esternalizzazione totale o parziale delle attività.
Qualunque sia la scelga, si deve riconoscere che la formalizzazione, la contrattualizzazione, l'imposizione di regole ferree e l'individuazione delle responsabilità in capo ad ogni soggetto coinvolto sono del tutto essenziali. I dettagli e le regole contenuti nell'atto di delega, la tipologia delle attività delegate e l'essenza dell'oggetto della delega, oltre che le circostanze specifiche, faranno di volta in volta propendere per l'una o per l'altra delle soluzioni sopra prospettate.

4. ESIBIZIONE

Dopo aver preso in considerazione l'intero complesso ciclo di vita del documento, durante il quale esso viene creato, memorizzato, archiviato, trasmesso e conservato, si deve ricordare che esso non può

essere per sempre dimenticato. Anche se sottoposto a conservazione legale, il documento potrebbe essere richiesto dal diretto interessato, dall'Autorità Giudiziaria, dalla Magistratura o da altri aventi diritto, a fini legali e probatori.
Buona parte dei documenti amministrativi e clinici prodotti in una Struttura Sanitaria contengono informazioni la cui comunicazione non può essere negata agli aventi diritto. Spesso sono proprio i pazienti i richiedenti stessi della consegna del documento conservato e, per il Codice in materia di protezione dei dati personali (D.lgs n.196/03), devono essere considerati le persone fisiche a cui si riferiscono i dati. Inoltre, l'art.84 del medesimo Codice asserisce che "I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato. 2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati".
Viene da qui sfatata la comune convinzione che la documentazione medica possa essere consegnata al paziente solo da un medico; basti leggere l'art.84 qui sopra riportato integralmente, da cui si comprende che incaricati formalmente individuati (amministrativi, sportellisti) possono essere delegati, dagli operatori sanitari principalmente preposti, a trasmettere i documenti contenenti i dati personali e sensibili direttamente ai pazienti interessati.
Anche l'art.50 del D.lgs n.82/05 conviene che la disponibilità dei dati deve essere garantita all'interessato: "1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati".

Ancora, la Deliberazione CNIPA n.11/04N impone all'art.6: "Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo." Il paziente, come qualsiasi altro soggetto legittimato, può quindi espressamente e formalmente richiedere ed ottenere dalla Struttura Sanitaria che la documentazione che lo riguarda gli venga consegnata; egli può inoltre pretendere anche che ciò avvenga su un supporto diverso da quello su cui la Struttura propone avvenga l'esibizione. Ma non solo, ciò deve avvenire previo pagamento di una somma da parte del richiedente.
Infatti, il D.lgs. n.196/03 afferma al comma 2 dell'art.10 che "Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica". Al comma 8 del medesimo articolo viene prevista la corresponsione di un adeguato

contributo: "Il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato".
L'Ufficio del Garante per la protezione dei dati personali, con l'art.3 della Deliberazione n.14/2004, sancisce che "Sulla base di una valutazione ponderata delle principali situazioni verificabili, e della circostanza che si tratta anche in questo caso di un contributo, va ritenuto congruo l'importo di euro venti. Si tratta di un importo massimo in quanto, anche in questo caso, il contributo non può comunque eccedere i costi effettivamente sostenuti e documentabili nel caso specifico". Nella Deliberazione il Garante si è spinto così a regolare i casi in cui l'interessato chieda che i propri dati siano posti su particolari "supporti di maggior costo quali audiovisivi, lastre, nastri o altri specifici supporti magnetici". Ma anche dove la gestione della documentazione è totalmente digitale, la richiesta di riversamento delle informazioni su supporto analogico da parte dell'interessato può divenire per la Struttura assai costosa in termini tecnologici, organizzativi e procedurali. E' da ritenersi, pertanto, che il pagamento di un congruo contributo, da determinarsi da parte della Struttura erogante la prestazione, debba prevedersi anche in caso di richiesta di riversamento dei dati da supporto digitale a cartaceo, anche se quest'ultimo è in effetti di costo irrisorio da un punto di vista materiale.

5. DOCUMENTI ORIGINALI E LORO COPIE

Qua e là nel testo sono già stati accennati dei concetti che riguardano la gestione degli originali e delle loro rappresentazioni (copie), da un punto di vista soprattutto organizzativo-funzionale. Qui vengono ripresi alcuni di tali concetti, a dimostrazione del fatto che una gestione mista della documentazione, fra digitale e analogica, è percorribile, sempre che i significati giuridici e legali risultino ben chiari e si dimostri una responsabile capacità di governo di tutti i flussi.
Nella tradizionale realtà sanitaria i documenti analogici prendono vita su supporto analogico che se necessario, viene sottoscritto autografamente in calce dal soggetto a ciò preposto (sia esso un medico, un amministrativo, un dirigente, etc. a seconda dell'ambito e delle competenze professionali). Il documento così formato in originale circola all'interno della Struttura, fisicamente accluso e allegato ad altra documentazione, oppure viene trasferito all'esterno, con consegna all'avente diritto. Ove vi sia obbligo di mantenimento nel tempo (come, per esempio, nel caso delle cartelle cliniche e dei documenti in esse contenuti, come i referti diagnostici, i verbali di Pronto Soccorso, le lettere di dimissione, etc.), i documenti in forma originale debbono rimanere all'interno della Struttura Sanitaria produttrice e lì sottoposti ad archiviazione legale analogica, sotto la responsabilità dei soggetti di volta in volta a ciò preposti a seconda della natura dei documenti stessi.
Per buona parte della documentazione clinica ciò viene espressamente previsto dalle vigenti norme in materia, e soprattutto dalla Circolare del Ministero della Sanità del 19 dicembre 1986, n. 61, la quale

impone alle Strutture Sanitarie pubbliche e private di conservare le cartelle cliniche di ricovero a cura della Direzione Sanitaria di presidio ospedaliero, unitamente ai referti, "illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario". Inoltre, secondo l'art.7 del D.P.R. n.128/1969 "Il primario è responsabile della regolare compilazione delle cartelle cliniche, dei registri nosologici e della loro conservazione, fino alla consegna all'archivio centrale". L'art.5 del medesimo decreto asserisce che il Direttore Sanitario "vigila sull'archivio delle cartelle cliniche, … rilascia agli aventi diritto, in base ai criteri stabiliti dall'amministrazione, copia delle cartelle cliniche".

La documentazione analogica che per legge deve essere sottoposta a mantenimento nel tempo presso la Struttura produttrice può essere trasmessa o consegnata a chi ne abbia diritto, ma solo sotto forma di copia (copia semplice o copia conforme all'originale, a seconda delle specifiche esigenze).
Vi è peraltro documentazione nata su supporto analogico (per esempio, il referto diagnostico per paziente ambulatoriale) che deve essere consegnata all'avente diritto in originale, senza obbligo alcuno per la Struttura di mantenerne una copia. Peraltro, spesso le Strutture gradiscono mantenere comunque presso di sé anche in quest'ultimo caso una copia analogica del documento, a meri scopi di consultazione clinica e di garanzia di reperimento delle informazioni.

Nel momento in cui si decide di avviare una gestione documentale, che voglia prevedere l'informatizzazione dell'intero ciclo di vita del documento, si deve fare molta chiarezza anche sulle eventualità di dover trattare le informazioni anche su supporto analogico, almeno per alcune porzioni di attività.
Oggi i documenti clinico-sanitari possono essere creati in forma nativamente digitale, eventualmente firmati con firma digitale, trasmessi e comunicati all'interno della Struttura produttrice come anche all'esterno, e successivamente sottoposti al procedimento di conservazione legale. L'originale, redatto informaticamente, deve continuare a rimanere nel luogo di archiviazione e poi di conservazione, mentre ciò che circola, sia in forma analogica sia in forma digitale, non è che una sua mera rappresentazione. Invero è doveroso richiamare ancora una volta il fondamentale art.43, co.3 del D.lgs n.82/05, il quale sancisce che "I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali". Un documento informatico, quindi, può essere trattato per parte del suo ciclo di vita in forma analogica, attraverso l'estrazione di copie, anche analogiche, dell'originale digitale; ma il mantenimento del tempo non può essere avviato che attraverso la conservazione legale.
Sia per l'originale sia per le eventuali sue copie deve essere individuato un ben chiaro valore legale, da determinarsi anche a possibili fini probatori di domani, che inevitabilmente andranno a modificare alcuni aspetti dell'iter organizzativo-funzionale, dai quali non si può prescindere.

6. DATA PROTECTION

Il concetto di tutela della riservatezza dei dati informatici è percepito solitamente come la limitazione della comunicazione e della divulgazione delle informazioni, grazie all'utilizzo di misure finalizzate ad impedire che la vita privata di un soggetto venga indiscriminatamente conosciuta o diffusa, così come il D.lgs n.196/03 e il suo Allegato Tecnico B - Disciplinare tecnico in materia di misure minime di sicurezza.

Ma oggi non ha senso alcuno voler approfondire la riservatezza del dato, anche con informativa sul trattamento e raccolta del relativo consenso, se il dato informatico non è trattato secondo la migliore e rigida sicurezza. Si può parlare di confidenzialità solo dopo aver approfondito le misure atte a dare certezza sulla sicurezza dei dati: vi deve essere garanzia che il dato esista (non possa essere colposamente o dolosamente eliminato) e che corrisponda al vero (non possa essere corrotto).

La tutela deve necessariamente passare attraverso l'analisi dei criteri funzionali e tecnologici da porre in essere per la conoscibilità delle informazioni solo dopo lo studio profondo delle regole per le loro integrità ed inalterabilità.

E' peraltro anche vero che spesso scomporre la sicurezza dalla riservatezza risulta assai difficile: solitamente dalla violazione delle regole della prima ne consegue quasi automaticamente la violazione di quelle inerenti la seconda e viceversa. Dimostrazione dell'importanza di questa impostazione logica e giuridica è data dall'*art.615 ter c.p.- Accesso abusivo ad un sistema informatico o telematico*, ove viene sancito che "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, e' punito con la reclusione fino a tre anni*". Il bene riservatezza dell'individuo, espressamente tutelato dal nostro ordinamento giuridico, viene leso quando qualcuno si introduce nel sistema informatico protetto da misure di sicurezza. Quindi anche per il codice penale presupposto della riservatezza è la sicurezza del dato e della sua gestione tutta.

6.1. GLI OBIETTIVI

Tavoli di lavoro a livello internazionale sono ormai concordi nel sostenere che, per giungere ad un accettabile livello di efficacia, le misure di sicurezza hanno l'obbligo di garantire il raggiungimento dei seguenti obiettivi:

- La **riservatezza**: vista come la prevenzione dell'utilizzo indebito di informazioni. Preservare la riservatezza significa ridurre, o addirittura eliminare, il pericolo che dei soggetti vengano a conoscenza di informazioni altrui senza esserne autorizzati. Tale salvaguardia deve presupporre che l'accesso ai dati sia sorvegliato attraverso quelle che vengono definite come *"minime"* ed *"adeguate"* misure di protezione.
- L'**integrità**: ovvero lo scongiurare modifiche e manipolazioni indebite dei dati. Assicurare

l'integrità significa, quindi, puntare ad escludere il rischio di perdita o modifica dei dati a seguito di malfunzionamenti dei sistemi, di non appropriato utilizzo degli stessi, all'interno e all'esterno la Struttura, sia colposo che doloso, di eventi naturali e non. Questo elemento risulta essere molto importante, poiché ogni alterazione dell'informazione nella sua consistenza logico-fisica non può che portare alla variazione del contenuto sostanziale dell'informazione stessa. Pertanto, proteggere l'integrità del dato significa anche assicurare la fondamentale correttezza del contenuto informativo.

- La **disponibilità**: deve essere interpretata come la garanzia dell'accesso al dato, in modo selezionato e controllato. Ciò può essere inteso come lo strenuo sforzo di prevedere ed evitare i pericoli di occultamento o di inaccessibilità ai dati durante un'attività del tutto lecita.

Accanto agli obiettivi della sicurezza qui sopra elencati, vanno inoltre approfonditi e posti in essere concretamente due elementi strutturali dei sistemi:

- La **verificabilità** e la **controllabilità** dei dati e delle attività svolte su di essi e nei sistemi in generale. Infatti. lo scopo qui è quello di identificare continuamente e con assoluta certezza attraverso gli aiuti tecnologici disponibili (audit trail, logging, audit file, identity management, ...) le operazioni compiute, gli autori di queste, le credenziali, i precisi momenti, gli ambiti. Ciò appare particolarmente importante sia per limitare le azioni ed i pericoli, ma anche per riuscire ad accertare i gradi di responsabilità ed i soggetti in capo ai quali tali responsabilità vanno individuate.
- La **definizione dei domini** è necessaria per la disponibilità dei dati da parte dei responsabili dei sistemi che li gestiscono, con completezza, aggiornamento ed esattezza.

Diventa, così, facile affermare che la sicurezza nella gestione delle informazioni non è un qualcosa che si aggiunge ai sistemi come un accessorio, bensì deve essere percepita come l'essenzialità del dato, cioè una sua caratterizzazione intrinseca.
La sicurezza nella sua molteplicità deve abbracciare tutti gli aspetti, fisico-logistici (es.: locali, accessi, strutture, materiali) informatici (es.: chiavi, cifrature, canali) ed umani (ruoli, identificazioni). La sicurezza nel trattamento informatico delle informazioni è dunque perseguibile soltanto impiegando le opportune misure organizzative-funzionali, tecniche e giuridiche.
Inoltre, è importante che tutte queste vengano ricercate ed implementate nell'intero sistema informativo e nei singoli sistemi informatici coinvolti. Ciò possibilmente sin dal primo momento della progettazione: infatti, se già si è detto che la sicurezza del dato è una sua caratterizzazione, è da evidenziare che le misure debbano quindi connotare l'architettura dei sistemi e vadano pertanto previste da subito, evitando modifiche e adattamenti in corso d'opera che rischierebbero di portare appesantimenti organizzativi ed economici.

E' comunque vero che la normativa vigente e la professionalità impongono di adottare le misure idonee anche ai sistemi già progettati e in uso, cercando un adeguamento attraverso provvedimenti adeguati.
L'evoluzione dell'Information and Communication Technology (ICT), con lo sviluppo di reti di interconnessione tra i sistemi informativi, oltre che la diffusione di applicazioni sempre più a largo spettro, suggeriscono un'attenta analisi ed impongono una rigorosa attenzione agli aspetti riguardanti la sicurezza e a quelli ad essa connessi. Condividere le informazioni, attraverso l'informatica e la telematica, sta diventando sempre più un'esigenza all'interno delle singole Strutture, fra le diverse Strutture, fra queste ed i cittadini. Ciò per garantire il dialogo, per accedere alle informazioni contenute nelle banche dati e per scambiarle, sia nell'ambito della Pubblica Amministrazione sia in quello privato.
Sta divenendo anche palese la fragilità del sistema intero e la sua potenziale pericolosità, se esso non riesce ad essere rigidamente governato. Quindi la sicurezza deve essere un elemento indispensabile nei processi di utilizzo dell'informatica come strumento professionale e anche in quelli di avvicinamento dei cittadini ai servizi a loro messi a disposizione. Invero risulta più che mai necessario fornire ora, sia agli operatori che ai fruitori dei servizi offerti, precise garanzie di sicurezza e riservatezza.

Gli ambiti della sicurezza e della riservatezza non devono riguardare isolati sistemi informatici o applicativi, ma devono permeare omogeneamente gli interi sistemi informativi di ogni struttura, oltre che quelli di connessione e collegamento fra diverse Strutture.

6.2. IDENTITY MANAGEMENT E AUDIT TRAIL

Da tutto ciò sin qui esposto in tema di data protection, si comprende bene che tutti i sistemi dovrebbero prevedere un servizio di Identity Management, e cioè di assegnazione al soggetto di un profilo (in funzione del suo ruolo nell'ambito della Struttura) e di identificazione nel momento in cui egli accede ed opera a vario titolo nel sistema informativo (sign-on dell'operatore). A seconda del proprio profilo, l'utente del sistema sarà autorizzato ad effettuare una serie più o meno ampia di operazioni sul sistema medesimo.
Tale procedura è peraltro da considerarsi parte sostanziale ed integrante dei provvedimenti imposti dall'Allegato B al D.lgs n.196/03 – Disciplinare Tecnico in Materia di Misure Minime di Sicurezza – e da includersi nel Documento Programmatico della Sicurezza (DPS) previsto dalle norme sulla sicurezza e la riservatezza nel trattamento dei dati personali.

L'esigenza di un'adeguata protezione del sistema da accessi non autorizzati, siano essi accidentali o intenzionali, impongono l'adozione di opportune misure finalizzate ad evitare il rischio di:

- distruzione o perdita, anche accidentale, dei dati
- accesso non autorizzato al sistema informativo
- trattamento non consentito dei dati o non conforme alle finalità della raccolta.

La progettazione di un sistema di sicurezza deve scaturire da un processo formalizzato di analisi del rischio che, oltre a considerare i rischi tipici, noti anche in letteratura e relativi a servizi esposti magari sulla rete, dovrà prendere in considerazione anche esperienze già realizzate di dimensioni confrontabili.
Le misure da adottare non possono essere esclusivamente basate sull'adozione di infrastrutture tecnologiche (Firewall e Intrusion Detection System), ma è necessario anche definire ed adottare un modello organizzativo mirato. Pertanto, si deve guardare ad uno specifico documento di definizione delle politiche di sicurezza, il cui contenuto, in linea con quanto richiesto dalle eterogenee Strutture coinvolte, deve andare a definire come minimo le seguenti componenti:

- i **ruoli**: l'insieme di responsabilità e di compiti che una o più persone debbono svolgere nell'ambito dell'organizzazione, onde assicurare il livello di sicurezza atteso;
- le **procedure**: l'insieme coordinato di azioni di varia natura, che coinvolgono più ruoli e che implicano responsabilità e vincoli di comportamento ben definiti;
- l'attività di **auditing**: l'insieme di controlli che dovranno essere svolti per assicurare il rispetto del livello di sicurezza atteso ed il rispetto dei ruoli e delle procedure previste nell'organizzazione della sicurezza
- il **monitoring** continuo.

L'operazione di sign-on, che per l'utente consiste nel fornire al sistema le proprie credenziali di autorizzazione, deve ovviamente essere annotata in modo automatico nel registro del sistema (servizio di auditing), corredata da un'accurata informazione su data ed ora dell'evento e dai riferimenti della stazione di lavoro su cui avviene l'accesso medesimo. E' evidente come divenga qui indispensabile operare trasversalmente, con un momento unico e sicuro di ogni attività posta in essere dall'utilizzatore dei sistemi, così come precedentemente raccomandato nel capitolo dedicato al tempo informatico.
Dopo una corretta attività di gestione delle autorizzazioni, il sistema deve prevedere l'adozione di procedure di strong-authentication basate su certificato di autenticazione a bordo di smart card, invece che su semplici username e password, del tutto incontrollabili ed aleatori.
Si sottolinea che non sempre l'operatore sanitario che utilizza il sistema sia un firmatario; quindi il suo ruolo potrebbe prevedere, secondo le policy inizialmente studiate e formalizzate nella Struttura, che egli possieda una smart card con a bordo il solo certificato di autenticazione, allo scopo di limitare e mappare le sue attività informatiche. Invece, se il ruolo dell'utilizzatore dei sistemi prevedesse anche che egli debba apporre la propria firma a documenti, la sua smart card dovrebbe essere completa sia di certificato di autenticazione, ai fini dell'identity management, sia di quello di firma digitale. Solo organizzando una rigida, ma sicura, gestione degli utilizzatori dei sistemi può essere garantita l'osservanza dei dettami normativi vigenti nazionali ed europei in tema di data protection.

Con l'adozione di tali procedure poi, i sistemi stessi potrebbero verificare, in fase del tutto preliminare, lo stato di validità dei certificati del singolo utente, interdicendogli addirittura l'accesso qualora i suoi certificati venissero trovati non in stato di validità, così come accennato ove si è parlato di 'potere di firma': in tale modo si eviterebbe anche fin dall'origine la possibilità che un utente, il cui profilo preveda l'utilizzo della firma digitale, possa procedere ad apporre la firma stessa su documenti digitali quando si trovasse in possesso di un certificato non più valido perché scaduto, sospeso o revocato.
E' pertanto qui che deve essere approcciato un vero e corretto metodo di gestione congiunto sia del 'potere di accesso' sia del 'potere di firma', con stretto riferimento alle imposizioni dell'Allegato B del D.lgs n.196/03, riguardanti i sistemi di autorizzazione dei profili degli utenti e della conseguente loro autenticazione.

Onde avere un senso tutto ciò che si è sin qui sostenuto in tema di sicurezza e riservatezza, oltre che di percorribilità di gestione delle scelte tecnologiche e funzionali intraprese, deve essere effettuato un continuativo e metodico **sistema di auditing**, in quanto ogni aspetto della gestione quotidiana del sistema informatico viene monitorato, in termini di accesso al sistema, di operazioni poste in essere, di documenti prodotti (ed eventualmente sottoscritti), di dati consultati, ecc. In altre parole è necessario essere in grado di rispondere con certezza ad alcune fondamentali domande, non solo per motivazioni organizzative, ma soprattutto medico-legali e probatorie: chi sei?, che cosa puoi fare?, che cosa hai fatto?.

Ancora una volta, viene evidenziato quanto sia importante che, per attuare puntualmente quanto detto, nell'ambito del sistema deve essere attivata una gestione sicura della **sincronizzazione del tempo** di tutti i sistemi coinvolti nella gestione dell'attività clinica, sanitaria e amministrativa, al fine di avere un riferimento temporale per ogni operazione compiuta e poter risalire con precisione alla sequenza temporale di tutti gli eventi e alla responsabilità individuale di comportamenti ed azioni di rilevanza clinica, amministrativa, medico-legale e probatoria.
Tutto quanto è oggetto di monitoraggio in base alle modalità sopra descritte viene tenuta traccia in un apposito **registro degli eventi.**

7. ANALISI DEI RISCHI E BUSINESS CONTINUITY MANAGEMENT

A conclusione in base a tutto ciò che è stato sin qui esposto, risulta evidente che tutti gli sforzi devono essere compiuti affinché gli incidenti informatici non si verifichino, adottando le opportune misure, sia a livello tecnico sui sistemi ICT sia a livello organizzativo-funzionale.
Tuttavia nei casi in cui l'incidente finisse ugualmente per verificarsi, appare estremamente importante che sia stato sviluppato e che sia pienamente operativo un piano che garantisca il più possibile la continuità dei servizi offerti dai sistemi ICT colpiti dall'incidente. A tale scopo è necessario che sia

sviluppato un *piano di Business Continuity*, per individuare tutte le misure atte a garantire la continuità dei processi dell'organizzazione, in funzione del loro valore e della qualità dei prodotti e dei servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.

Gli operatori sanitari addetti all'utilizzo dei sistemi ICT, che trattano informazioni e applicazioni rilevanti dal punto di vista della sicurezza ICT, e soprattutto il personale che ricopre i ruoli di gestione della sicurezza ICT, devono anche essere attentamente formati e poi selezionati per determinate attività, sulla base di criteri di affidabilità e competenza, in modo da rendere il più possibile basso il rischio che tale possano essere compiute, intenzionalmente o accidentalmente, azioni che compromettano la protezione delle informazioni e applicazioni.
Nel contempo è importante che il personale sia comunque messo nelle condizioni professionali di svolgere al meglio i propri compiti, dotandolo delle risorse e del supporto necessari e consentendogli la fruizione di un adeguato piano di formazione e sensibilizzazione anche nell'area della sicurezza, oltre a dover essere garantita un'alta motivazione del personale, preferibilmente istituendo ruoli specifici per la sicurezza ICT.

Ogni struttura che desideri provvedere allo sviluppo di adeguate politiche di gestione documentale nella maggiore liceità e sicurezza dovrà necessariamente rifarsi ad una metodologia di analisi del rischio. Quest'ultima va vista come il processo fondamentale per identificare i pericoli e fissarne la portata. Ovvero, l'analisi del rischio è quel processo che definisce le esigenze di sicurezza nell'utilizzo dell'ICT in un'organizzazione, ed individua le opportune soluzioni di verifica e governo, pianificando, realizzando e gestendo i propri sistemi.

7.1. ANALISI DEL RISCHIO

Senza una continua e stabile valutazione della portata del patrimonio informativo, dell'intensità dei pericoli, delle vulnerabilità dei sistemi e dei potenziali impatti sull'attività della Struttura (che, come più volte sottolineato, è protesa a garantire la salute dei cittadini), può apparire difficile calare la teoria normativa nella pratica quotidiana, rispondendo alle esigenze di un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni che potrebbero realizzarsi.
Nei nuovi complessi sistemi sempre più aperti, cooperanti, ed interoperabili, i confini continuano a divenire sempre più vulnerabili, evidenziando la necessità di un continuo processo di analisi e di gestione del rischio, conformemente agli standard nazionali ed internazionali. L'obiettivo, quindi, dell'analisi è rappresentato dalla capacità di approfondire l'ambito dei potenziali rischi, individuandoli, classificandoli e valorizzandoli, concordando infine quali sono le misure idonee a ridurre la debolezza dei sistemi, con proporzionale garanzia di sicurezza nell'erogazione dei servizi.

Che si voglia parlare di gestione documentale pura, come di data protection (peraltro questa del tutto amalgamata con la prima), l'analisi del rischio deve essere ormai intesa come una parte essenziale e propedeutica all'adozione di efficienti sistemi per una sicurezza generale ed omogenea. Per giungere a ciò, secondo i cultori della materia, i seguenti passaggi non devono essere trascurati:

- identificazione e valutazione degli asset informativi;
- assessment dei pericoli e delle vulnerabilità;
- rilevamento dello stato esistente e pianificazione dei controlli;
- risk assessment;
- accertamento e selezione dei controlli e riduzione dei rischi;
- accettazione del rischio.

L'analisi del rischio ed i conseguenti risultati contribuiscono, anche, ad aumentare la consapevolezza della Struttura intera dell'esistenza di alcune problematiche, e soprattutto porta alla sensibilizzazione per l'adozione di un'intelligente pianificazione.
Gli approfondimenti così impostati forniscono le facilitazioni per percepire i potenziali pericoli della mancanza o del cattivo uso dei mezzi e dei sistemi, ed aiuta nella individuazione delle congrue misure da porre in essere.

8. ALLEGATO A

Questo allegato ha l'intento di esporre in modo didascalico quanto precedente emerso attraverso la raccolta dei dati, mediante il questionario di ricognizione sulla firma digitale.
Il medesimo ha avuto lo scopo di fare il punto della situazione nelle ULSS dell'area vasta veneziana, permettendoci di capire quanto ci fosse di già attivo e in quale modalità, riguardo la firma digitale e le sue apparecchiature e i suoi applicativi. Il questionario ha cercato di essere il più esaustivo e dettagliato possibile, entrando nello specifico della situazione, con domande ad hoc che riguardassero gli ambiti dove fosse usata la firma digitale, quale formato venisse utilizzato, il volume dei documenti prodotti, le metodologie per l'archiviazione e quelle per la conservazione sostitutiva.

Oltre al questionario, sono state effettuate delle visite in ogni ULSS dove si è analizzato il questionario compilato, in modo che esso fosse il più preciso possibile e non contenesse risposte errate, tali a causa, probabilmente, della poco approfondita conoscenza dell'argomento trattato. Le visite hanno avuto anche lo scopo di portare ulteriore chiarezza sull'argomento, eliminando eventuali dubbi o cattive abitudini acquisite. Inoltre, ci si è prefisso lo scopo di dare una conoscenza precisa e omogenea ad ogni ULSS coinvolta, in modo da poter finalmente partire tutti con lo stesso livello di preparazione e conoscenza.

In questa fase è stato possibile anche raccogliere del materiale e delle informazioni ulteriori, sempre utili e proficue.

Abbiamo vari esempi:

- in alcune realtà è emerso come, al momento in esame, coesistano diversi protocolli contemporaneamente nella stessa ULSS; è evidente come ciò stia creando dei disagi in una fase ancora precedente all'apposizione della stessa firma digitale o all'archiviazione del documento firmato.
- si è riscontrata in varie ULSS l'abitudine di passare allo scanner i documenti ancora in formato analogico, con l'errata idea che facendo in questo modo si ottenga un documento in formato digitale. Questa erronea credenza conduce evidentemente a dei risultati sbagliati. Tale pratica porta con sé solo il vantaggio di ottenere delle rappresentazioni digitali degli originali cartacei, in modo che le rappresentazioni siano sicuramente di più facile e veloce reperimento, ma non sostituiscano in nessun modo il documento originale cartaceo;
- in una realtà abbiamo addirittura riscontrato la volontà e necessità di implementare al più presto il processo di firma digitale e archiviazione e conservazione, poiché utile per avviare altri nuovi servizi, come la possibilità di consultare i referti on-line;
- è stato constatato che alcune realtà molto piccole sono, invece, già attive negli ambiti amministrativi, con processi già quasi interamente completati in svariate fasi;
- lo studio è stato condotto sulle seguenti 6 ULSS che compongono l'area vasta veneziana: ULSS10 San Donà di Piave, ULSS12 Veneziana, ULSS 13 Mirano, ULSS14 Chioggia, ULSS18 Rovigo,

ULSS19 Adria e i dati raccolti sono stati aggiornati a fine settembre 2009, e successivamente elaborati nel mese di ottobre 2009.

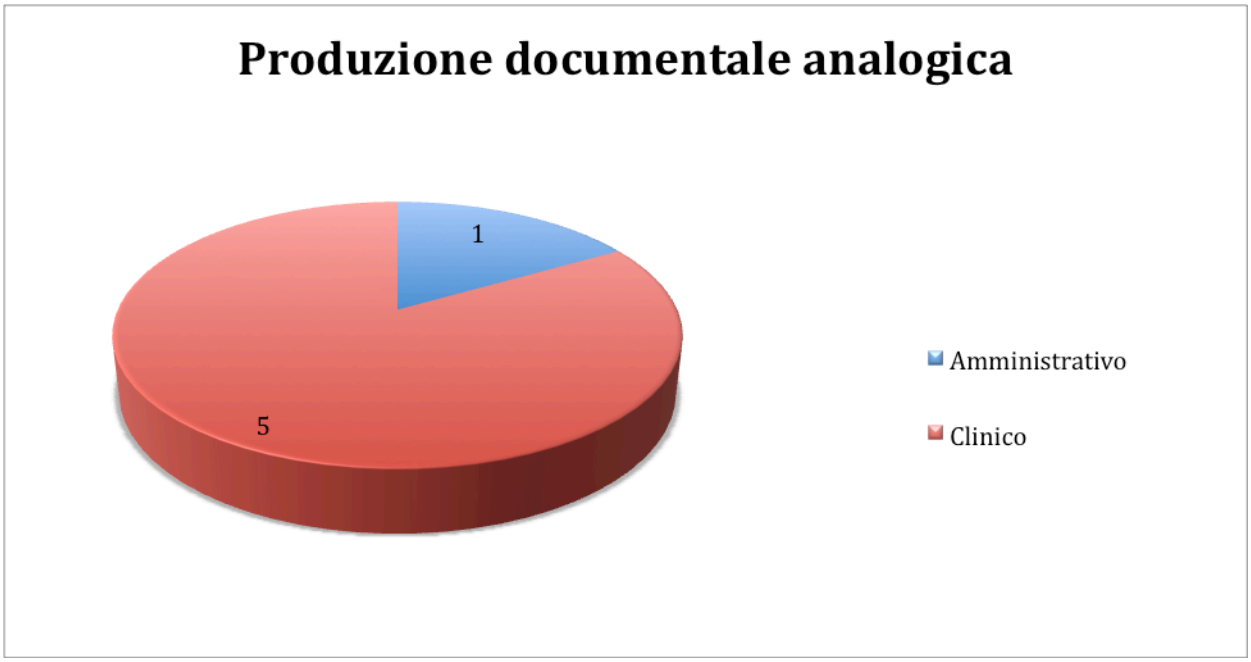
Il dato principale che appare dopo una prima rapida analisi è senza ombra di dubbio la totale disomogeneità che regna in quest'area vasta, riguardo l'argomento in oggetto. Tale discontinuità risulta dal fatto che le 6 ULSS coinvolte non hanno gli stessi obiettivi, né metodologie, né gli stessi servizi implementati. Con certezza possiamo già affermare che esse non sono né allo stesso livello in quanto a dotazione tecnologica, né allo stesso livello per gli strumenti già in uso, né tanto meno le stesse regolamentazioni.

Per dovere di cronaca e per una maggiore chiarezza, prima di proseguire con l'esposizione dei dati raccolti e analizzati, si chiarisce che ogni risultato sarà seguito dal relativo diagramma, al fine di avere una visione più immediata dei risultati raccolti.

Ora, cominciamo ad addentrarci finalmente nello specifico dei risultati raccolti mediante il questionario compilato dalle ULSS coinvolte.
L'osservazione iniziale ci porta subito ad una conferma della prima impressione avuta, e quindi della disomogeneità che regna, come unico fil rouge, lungo tutto lo studio fatto sull'intero questionario sottoposto.
Se per alcune domande noteremo una certa omogeneità delle opinioni fornite poi scopriremo, magari all'interno di una singola risposta di una stessa domanda, una totale eterogeneità, che ci ricondurrà sempre al risultato principe che nasce dallo studio dell'osservatorio.

Iniziamo, appunto, con le osservazioni suggeriteci dall'analisi del questionario, che fin da subito ci confermeranno la tesi della eterogeneità dei risultati.

La prima considerazione che emerge è che, mentre la quasi totalità delle ULSS sotto analisi si trovi d'accordo nell'affermare che ognuno di loro ha la maggior produzione documentale di tipo analogico nell'ambito clinico, e solo una piccola minoranza ha la maggior produzione nell'ambito amministrativo. Poi c'è, invece, un frazionamento quando andiamo ad analizzare la tipologia di documenti prodotti, siano essi clinici o amministrativi, che si dividono in tantissime tipologie, diverse per ogni ULSS chiamata in esame.
Questa la prima analisi, con la suddivisione tra produzione documentale clinica e amministrativa.



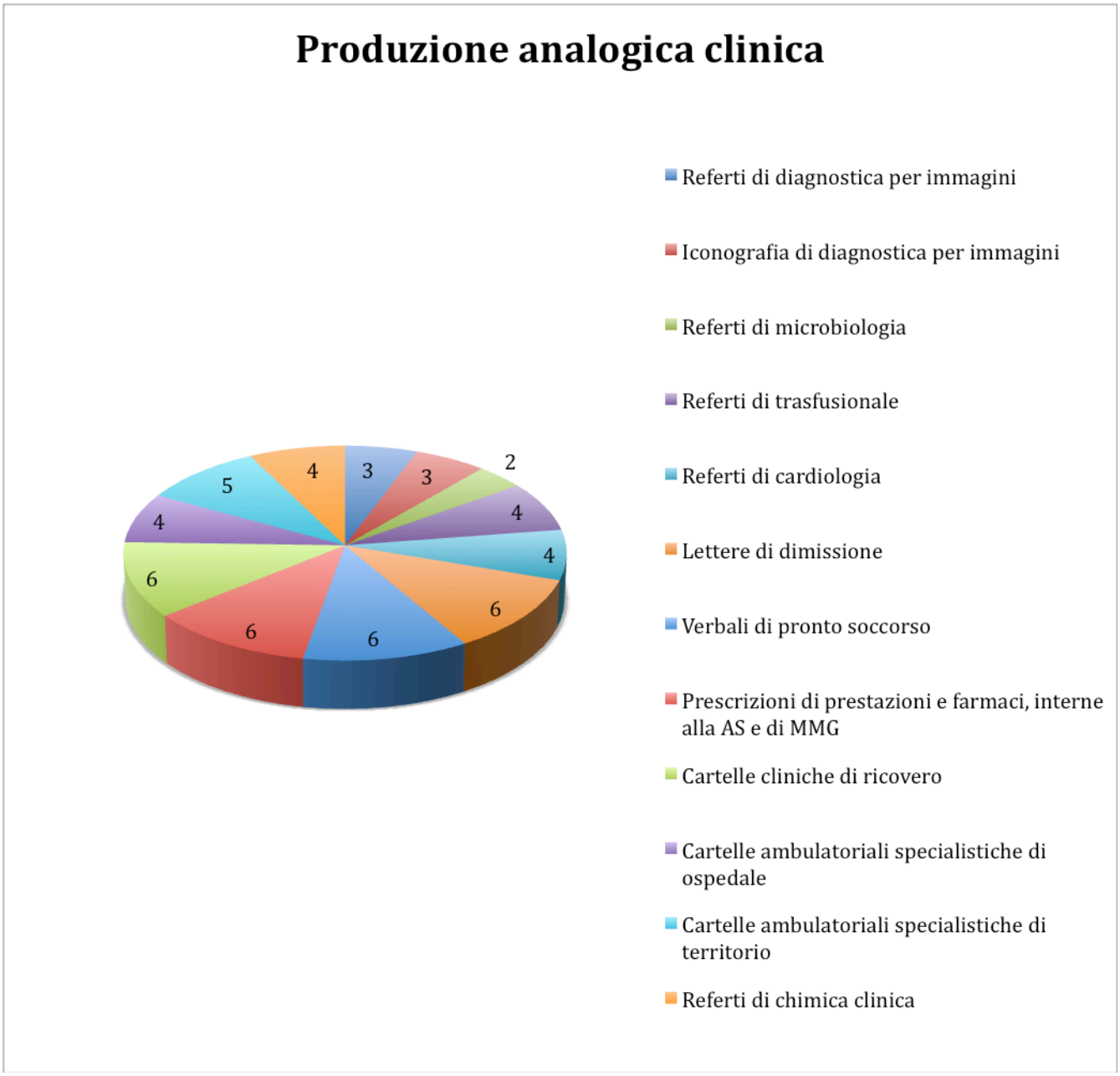
Se, difatti, pian piano si scende nello specifico e si analizza la tipologia di produzione documentale amministrativa analogica annua, la tendenza è quella di occuparsi, nella quasi totalità dei coinvolti - soprattutto e in ugual misura - di documenti del tipo delibere, mandati di pagamento e fatture e, sicuramente, in modo meno massivo di altri tipi di documenti come, ad esempio, circolari direzionali o altro.

Si evince dall'analisi, in modo piuttosto basilare, come la tendenza sia chiaramente quella che, al giorno d'oggi, ancora una grossa parte della produzione di documentazione amministrativa sia analogica, e che quindi, il lavoro da compiere verso la completa digitalizzazione di questa sarà di una certa entità.

Ciò che, ancora una volta, infonde delle perplessità è come non sia presente un fronte unico su cui agire all'unanimità in tutte le sei ULSS, ma come il bisogno sia quello di personalizzare su ognuna di loro il relativo servizio: si presume quindi, che ipotizzando il momento in cui il servizio di dematerializzazione potrebbe veder l'avvio, sicuramente avremmo dei servizi diversificati; ovvero, a seconda della ULSS che andremmo a prender in esame, ciascuna si troverebbe ad avere una necessità diversa, che la costringerebbe ad attivare in primis un determinato servizio in una ben specificata specialità o reparto, che non necessariamente risulti lo stesso della ULSS attigua.

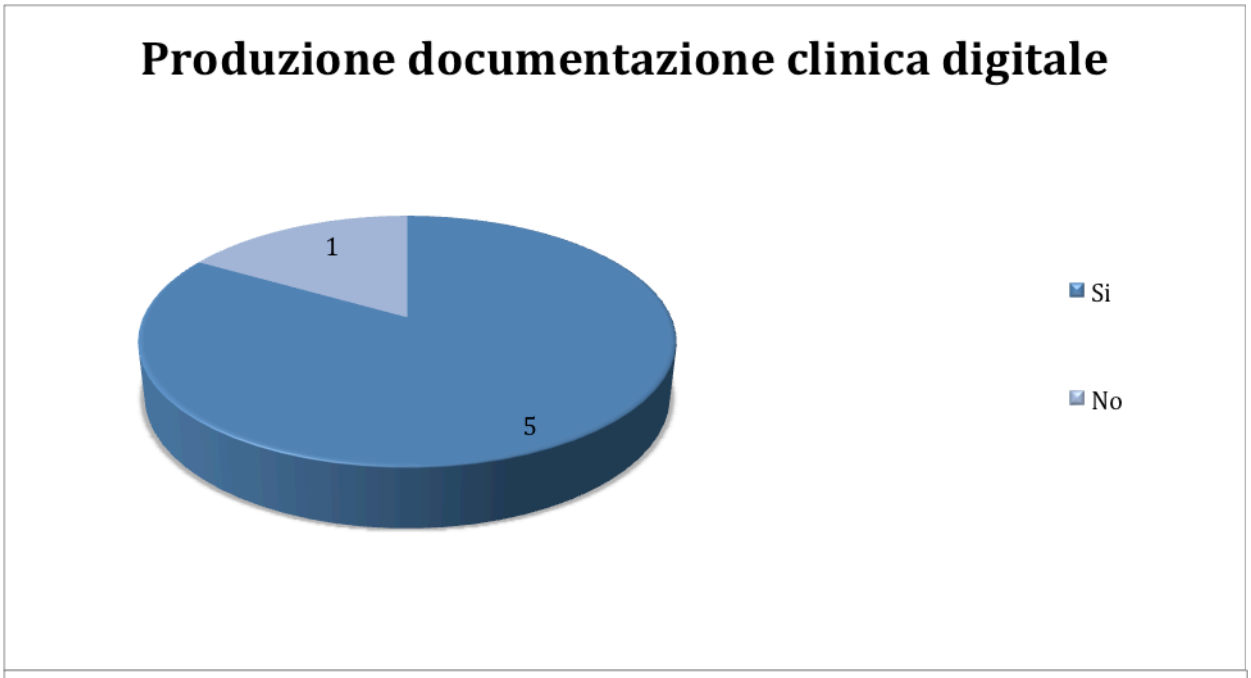
Proseguendo con l'analisi di quanto prodotto circa la documentazione analogica clinica, il frazionamento appare ancora più evidente, svelando che la totalità delle ULSS produce tale tipologia di documentazione, soprattutto per quanto riguarda l'ambito delle prescrizioni (siano esse prestazioni o farmaci), le cartelle ambulatoriali, i referti di chimica clinica e cartelle cliniche di ricovero, rispettivamente in ordine decrescente. Queste, per ora, si sono dimostrate le aree e gli ambiti di maggiore interesse e rilievo in quanto a volumi prodotti, quindi parrebbero, a tutto diritto, essere i primi reparti fra i candidati per la futura implementazione dell'intero servizio del ciclo di digitalizzazione, o dematerializzazione che dir so voglia.

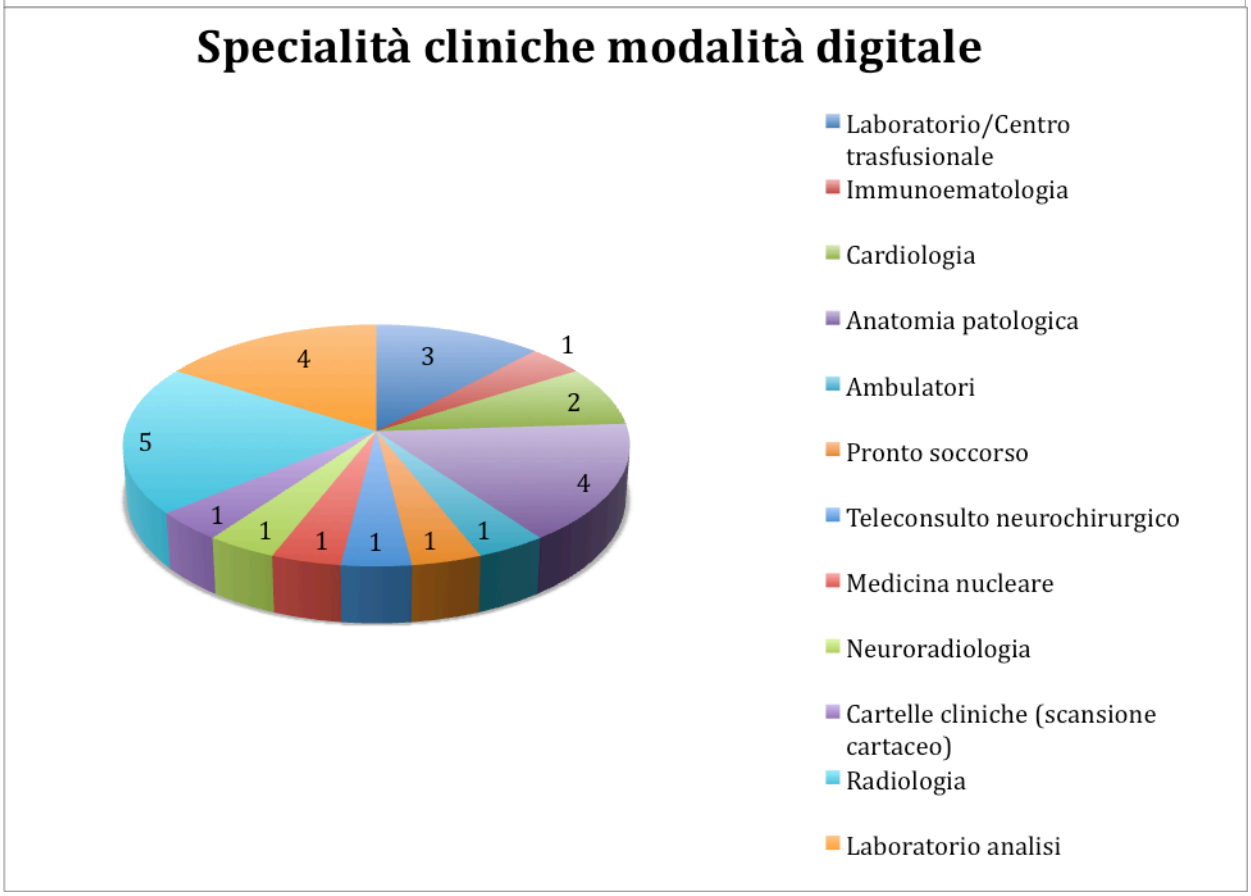
Soffermandosi al solo ambito delle prescrizioni, si nota come la grossa mole di documenti che al momento esistono e vengono tuttora generati in modalità analogica, e che certamente in un futuro molto prossimo dovrebbero essere gestiti in digitale, sarebbe almeno una media di oltre 1.000.000 di documenti l'anno, altri 200.000 sarebbero da considerare con le cartelle ambulatoriali, altrettanti con i referti di chimica clinica, altri 30.000 per le cartelle cliniche di ricovero e via con numeri consistenti anche in tutti gli altri settori considerati (ben 12, per ora, i papabili per il passaggio da analogico a digitale).



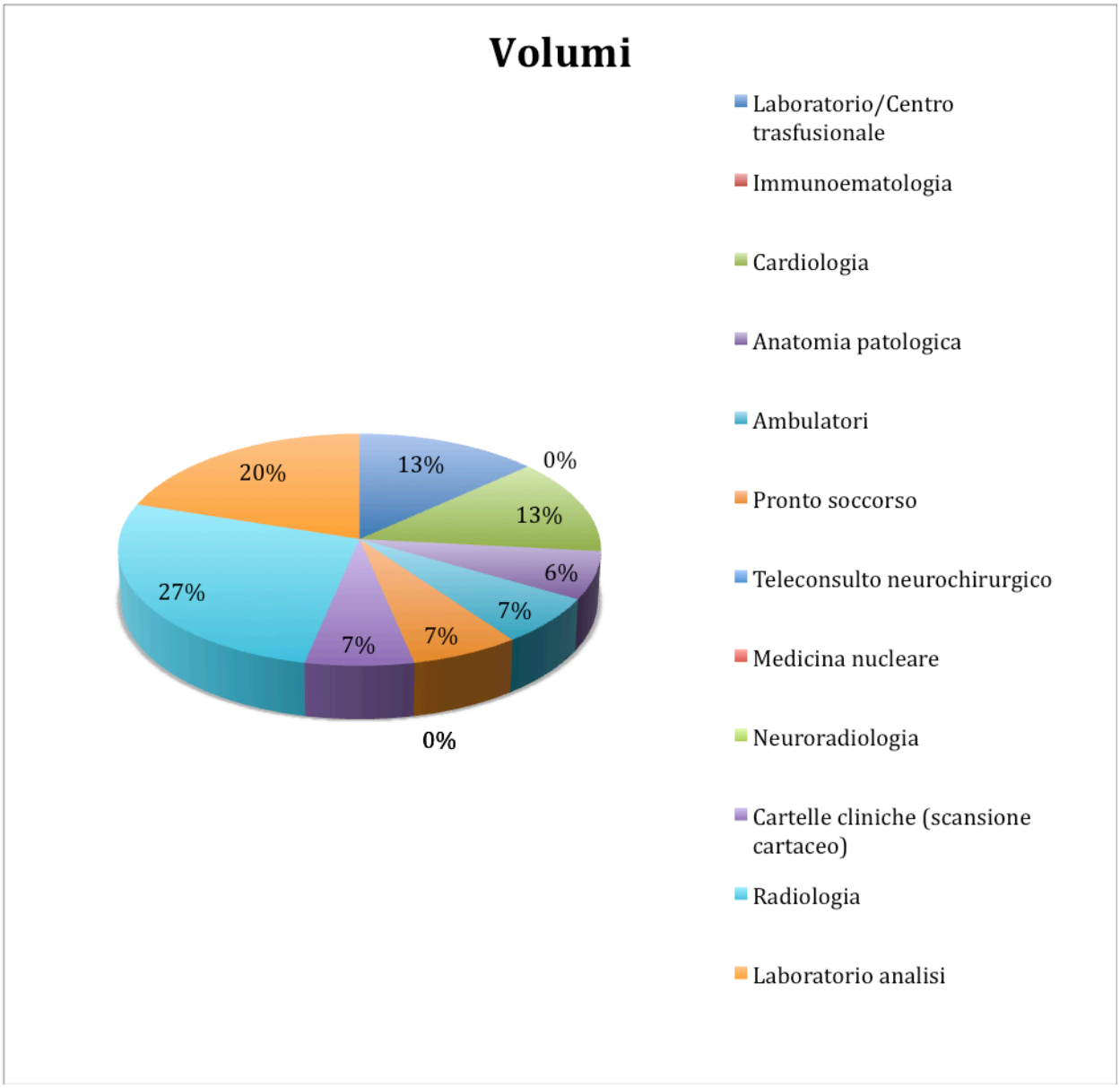
Addentrandosi sempre più nell'indagine, dal questionario deriva che la quasi totalità degli intervistati dichiara di produrre già ora dei documenti clinici in formato digitale, soprattutto documenti che riguardino i referti (la fetta più consistente tra le varie specialità entrate in gioco), in special modo di tipo iconografico, ma è anche vero che, al momento, nella produzione già esistente, in questa babele di numeri, volumi e specialità, le più differenti, ogni ULSS e ancor meglio ogni reparto all'interno di ciascuna ULSS, produce i documenti con specifiche applicazioni che sono le più varie, tanto per citarne alcune: Metafora, Sigma, MEDarchiver, Exprivia, RA2000, TD-Sinergy, Emonet, Windopath, GE, DedaGroup, Dacos srl, Noem alife, Ebit, ItalTBS, Esaote, per completezza. Questa enorme differenziazione, pur non producendo complicazioni sostanziali al momento, in un secondo tempo andrà di sicuro soppiantata da

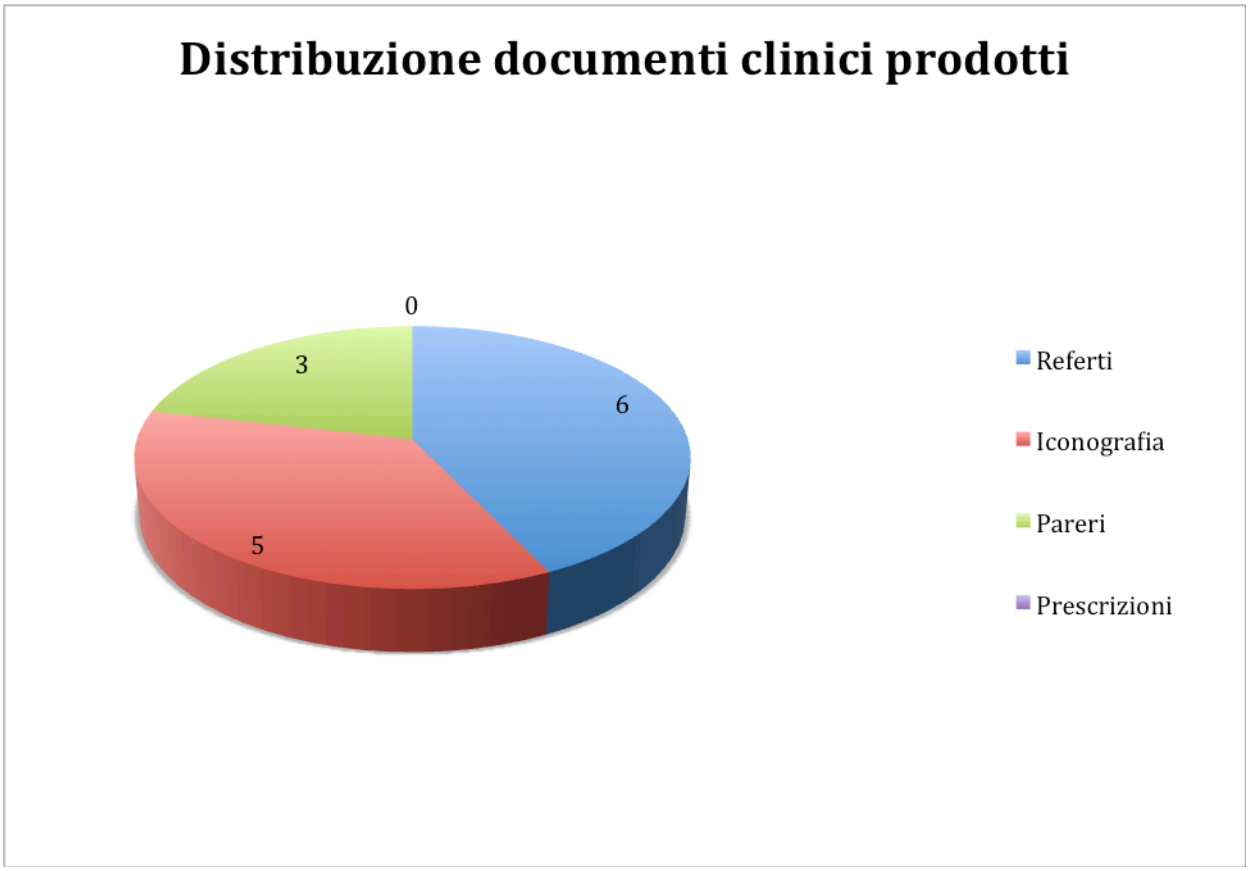
un sistema più uniforme, uguale per tutti i reparti coinvolti, con l'intento di ridurre le possibilità di errore e di interoperabilità.





Dall'analisi dei volumi della documentazione digitale clinica si percepisce quale sia l'andamento generale: valutando velocemente i reparti che cubano le moli maggiori, si evince come mentre si va ad implementare già il singolo e solo reparto di radiologia, l'entità di documenti che verrebbero gestiti in digitale sarebbe almeno una media di 150.000 documenti l'anno, altri 50.000 con l'anatomia patologica, oltre 200.000 con il laboratorio analisi, e di seguito le restanti specialità, ognuna con numeri di tutto rispetto.

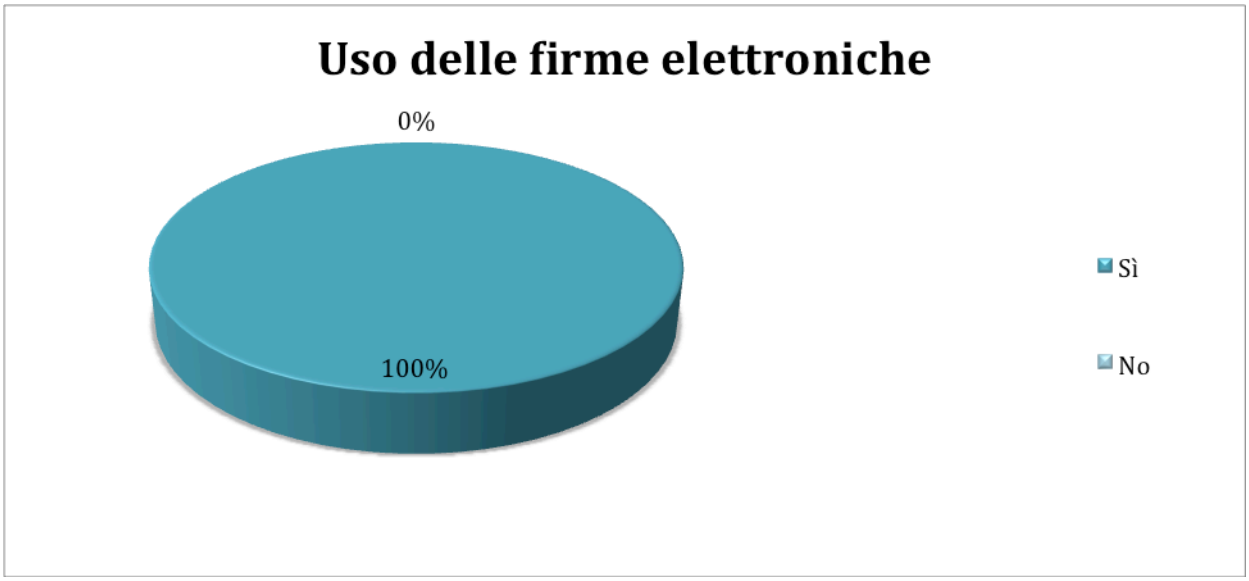


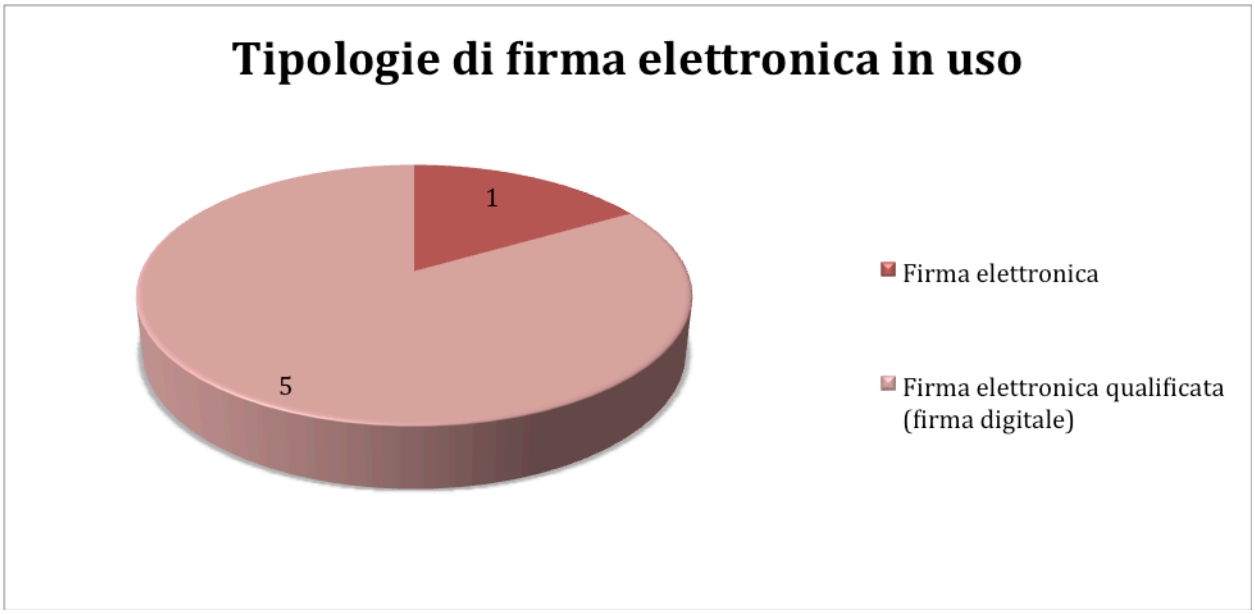


Se fino a qui il quadro è a tratti frammentario e in alcuni altri, invece, sembra quasi essere più omogeneo, da questo punto in poi, la situazione va nettamente peggiorando.

Nel momento in cui si vanno ad analizzare nel dettaglio i passi successivi del processo, composto da firma, archiviazione e conservazione sostitutiva, tutto diventa nettamente più confuso, in quanto si evidenzia il fatto di quanto non fossero ben chiare le norme e le modalità per compiere determinate azioni, al fine di portare a termine l'intero processo in modo corretto.

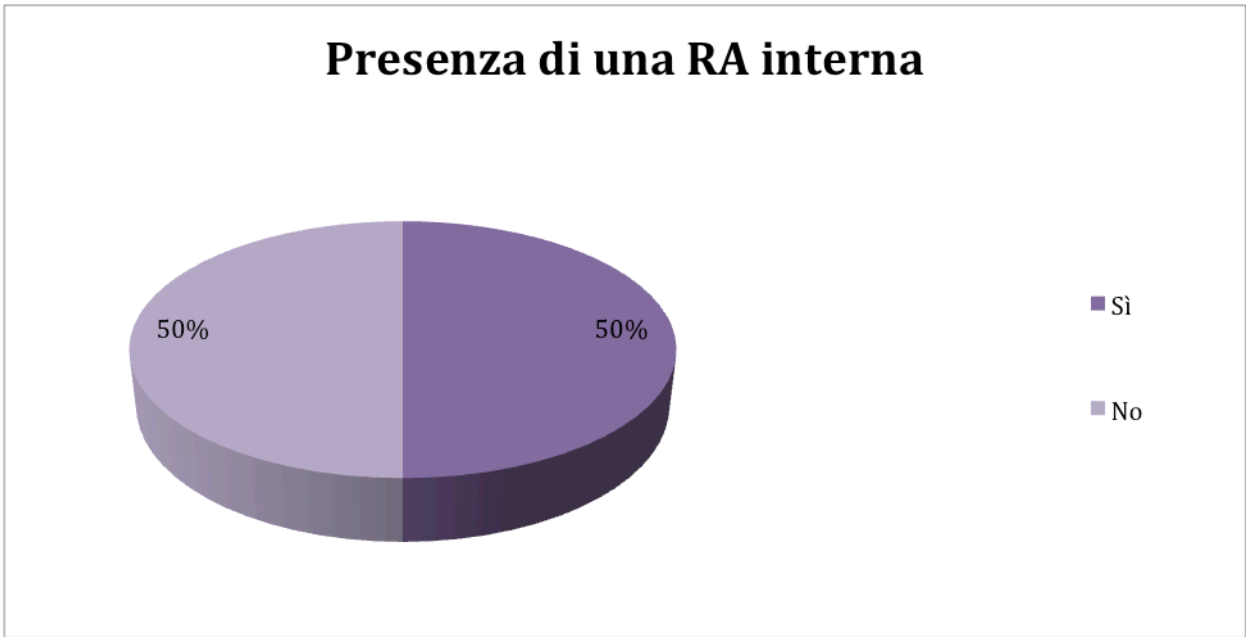
Per quanto concerne l'uso della firma elettronica, tutte e 6 le ULSS dicono di averla già in uso, ma poi si scopre come, in realtà, qualcuno usi ancora una semplice firma elettronica e altri, invece, quella elettronica qualificata, ripartita a sua volta in modo diseguale tra le varie tipologie disponibili, poiché si nota l'impiego sia della firma di tipo PKCSk#7 e sia quella PDF, che risultano essere ormai soluzioni obsolete e sorpassate: nessuno invece ha ancora implementato la soluzione più nuova, completa e versatile, cioè quella di tipo XML, che è poi l'unica soluzione proiettata al futuro, almeno per ora.

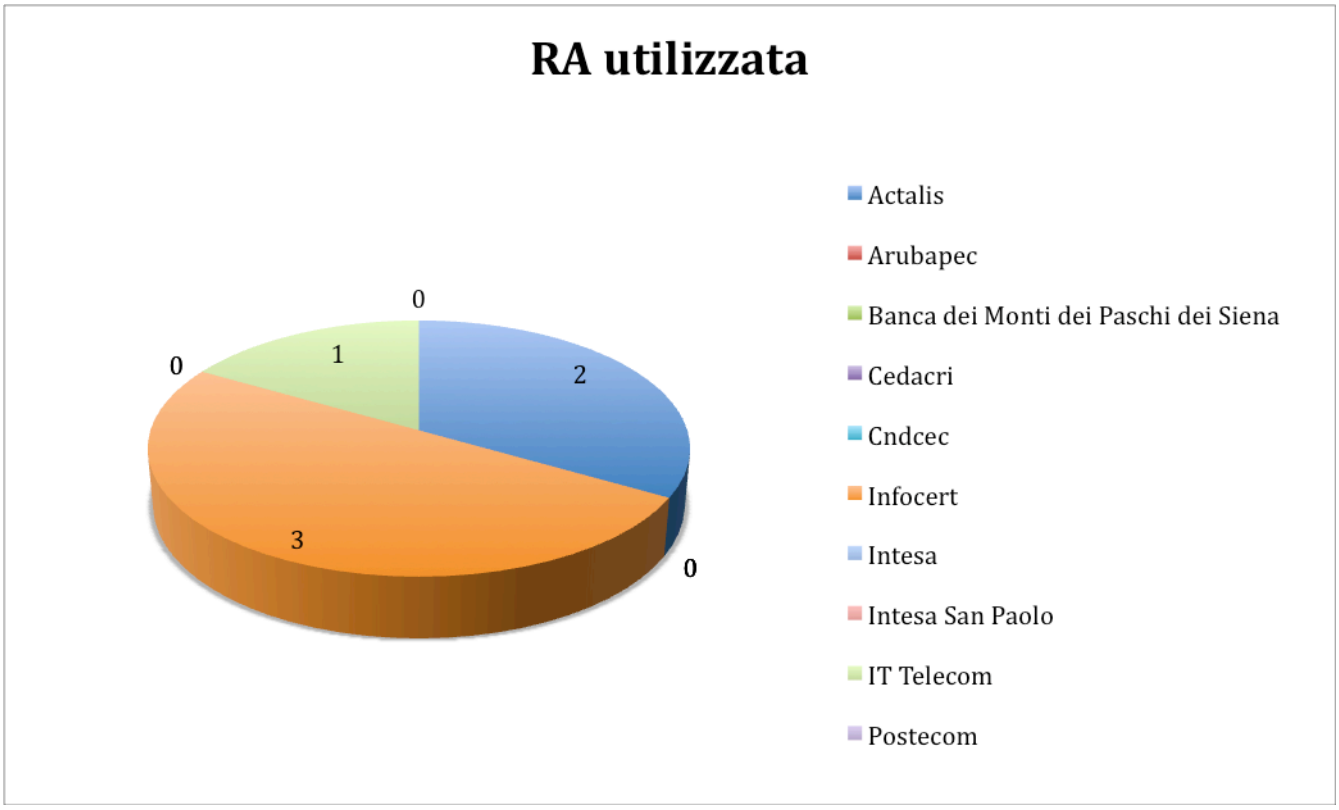

Uso delle firme elettroniche
0%
100%
Sì
No


Tipologie di firma elettronica in uso
1
5
Firma elettronica
Firma elettronica qualificata (firma digitale)


Tipologia di firma digitale in uso
0
1
4
Pkcs#7 (p7m)
PDF
XML

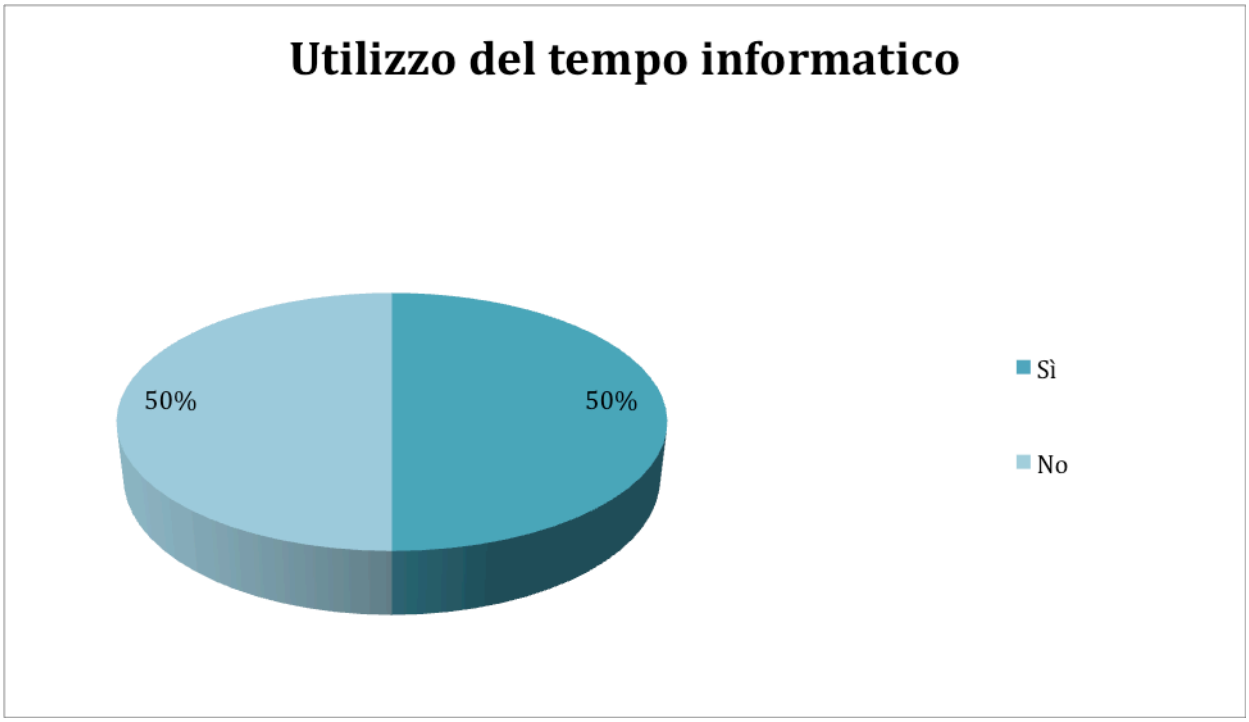
Procedendo passo a passo nel percorso di firma, archiviazione e conservazione sostitutiva, ci imbattiamo successivamente anche nella tematica della Registration Authority, e ancora una volta dal questionario deriva che solo la metà delle aziende abbia già provveduto ad organizzarsi con una R.A. interna all'azienda, e tra queste poche ci si suddivide, di nuovo equamente tra le varie ditte presenti come Actalis, IT Telecom e Infocert; ma il dato più sconcertante è che alcune ULSS adoperino più di una R.A. all'interno della stessa azienda, e non la medesima per l'intera struttura.
Questo rimane sicuramente il dato più emblematico di questa tanto ribadita disomogeneità: passi che all'interno di una singola azienda si abbiano magari firme di tipo diverso, o differenti fornitori, ma il fatto che, all'interno di una stessa ULSS non si riesca nemmeno ad avere un'unica R.A., la dice lunga.
Certo che, come coesistono varie realtà ora, tanto meglio potranno continuare a coesistere per il futuro, ma ciò non è di aiuto per l'idea di standardizzazione e interoperabilità ampiamente auspicata.





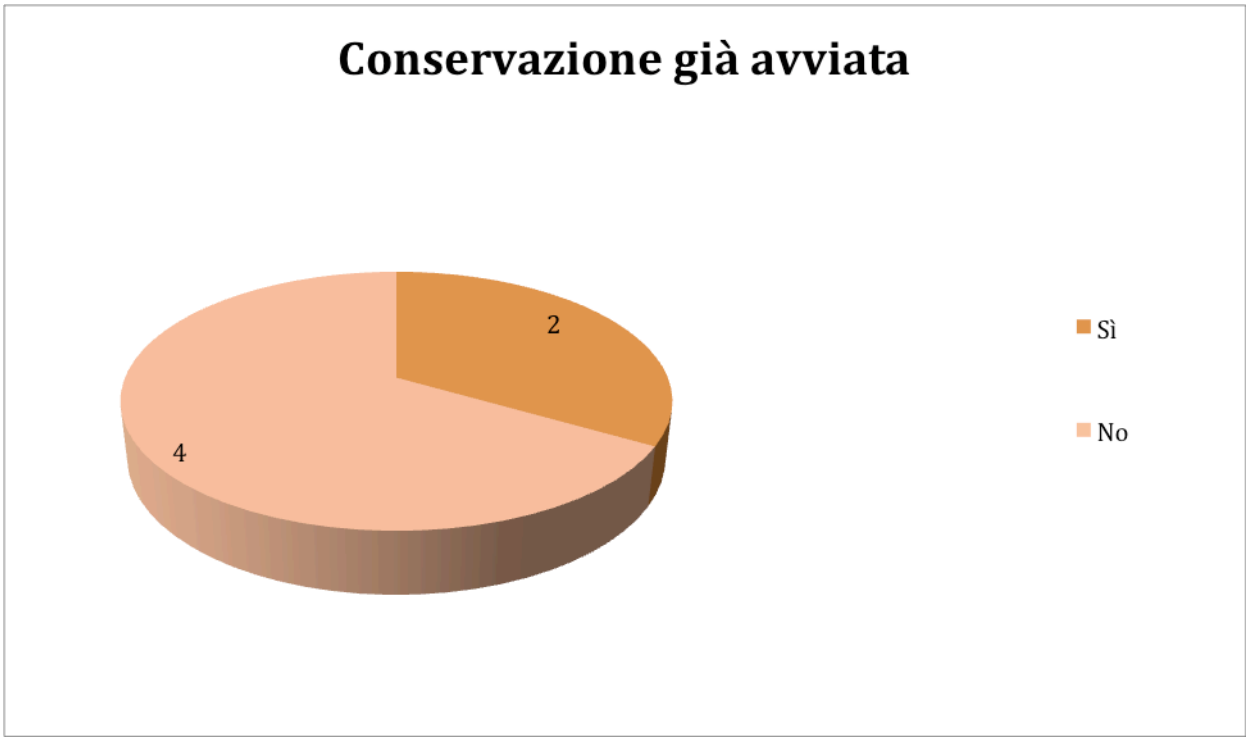
Arrivati a questo punto, non ci sconcertiamo più di fronte a qualsivoglia risultato. Ancora una volta ci si ritrova davanti ad una nuova frammentazione quando andiamo a parlare di tempo informatico, riferendoci alla marca temporale apposta sul documento: neanche a dirlo, è usata, come ormai di consuetudine, solo dalla metà degli interrogati, i quali si diversificano ulteriormente, come è ormai ovvio che sia, nel modo di apporla al documento informatico.

Come se non bastasse, si verifica anche il caso che qualcuno usi in modo improprio questa metodologia, creando, di fatto, un documento che non e' realmente marcato temporalmente, con tutte le conseguenze del caso, che ciò comporta; ci ritroviamo fra le mani un documento che non è più generato e mantenuto a dovere, quindi non ha più valore medico-legale al 100%, e non è più opponibile ai terzi.


Utilizzo del tempo informatico
50%
50%
Sì
No

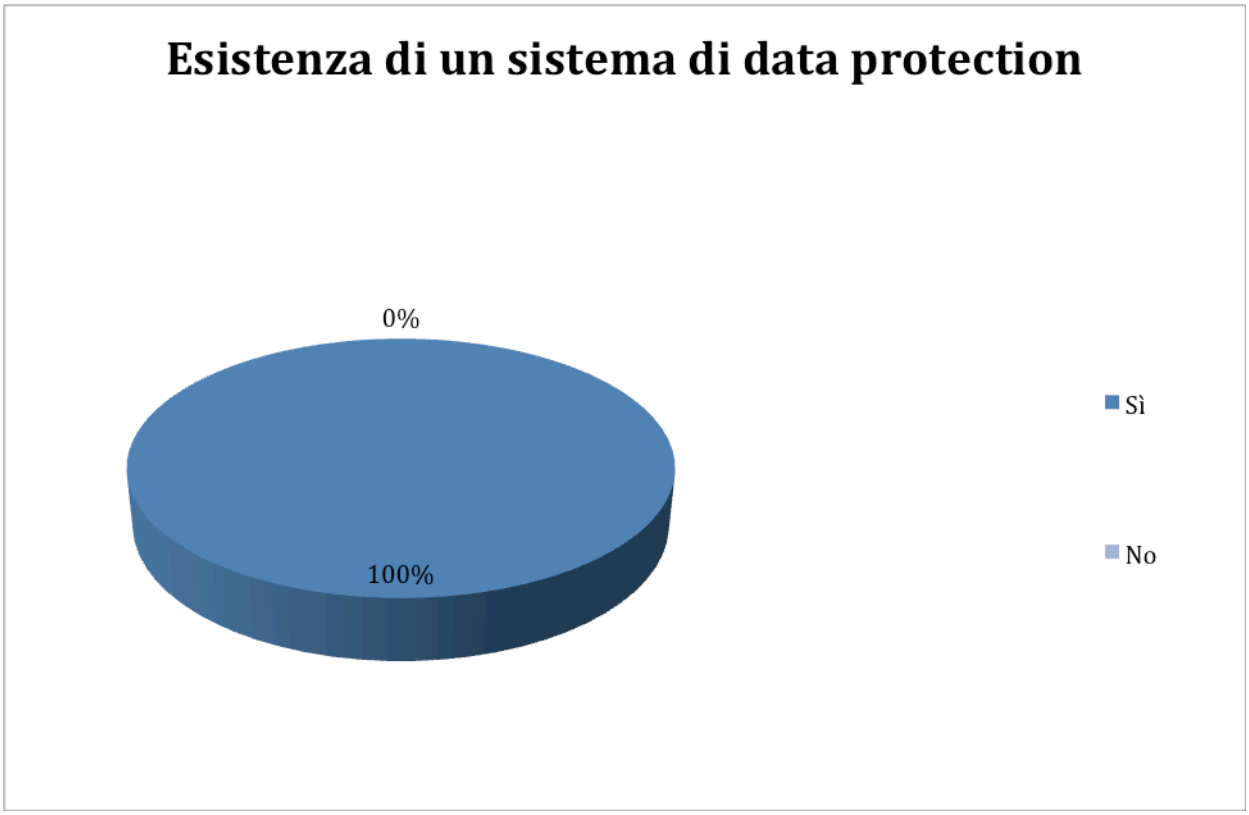

Apposizione del tempo informatico
1
1
4
Apposto direttamente al documento informatico
Dato non pertinente
Dato non disponibile

Facendo un passo ulteriore e spostandoci questa volta nell'ambito della conservazione, troviamo una risposta positiva solo da parte di 2 attori sui 6 coinvolti, quindi solo 2 hanno già avviato un processo di conservazione sostitutiva.
Inoltre, dei soli 2 che rimangono in gioco, uno purtroppo opera in modo non corretto e risulta, infine, che l'ultimo e l'unico attore che a questo punto non sia stato eliminato, non ha provveduto all'individuazione e alla nomina di un addetto alla conservazione, rendendo quindi, ancora una volta, non valido il lavoro fatto fin'ora.

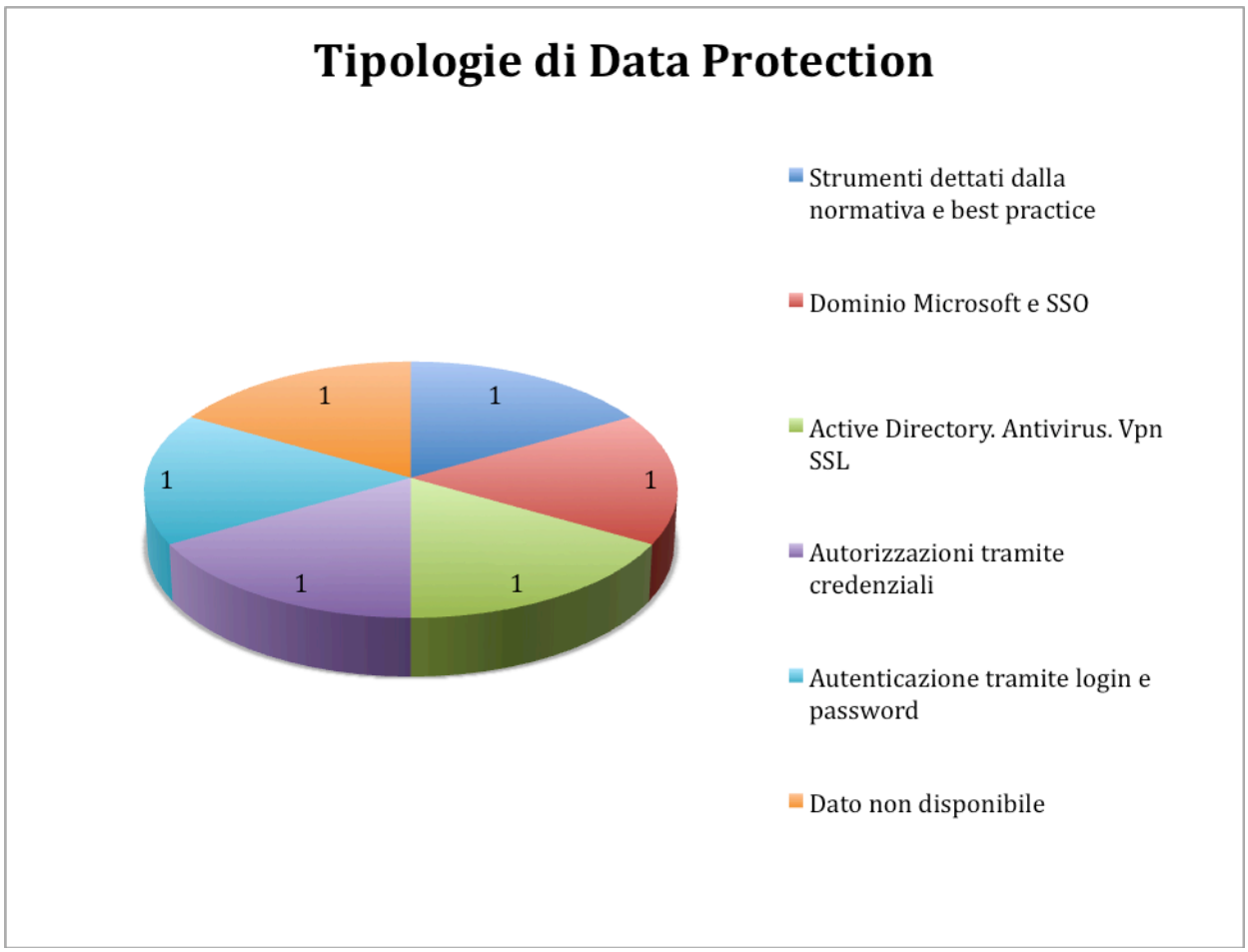


Arrivati a questo punto verrebbe da pensare che stando così le cose, dei 6 partecipanti in gara inizialmente, al momento nessuno sia rimasto in gioco, con le carte in regole, viste le modalità con cui hanno eseguito i passi necessari per i processi da svolgere; invece, sorprendentemente, arriva l'ultimo dato raccolto: tutti affermano di avere un sistema di data protection, che includa sicurezza e privacy, gestione delle autorizzazioni e delle autenticazioni ai sistemi, comprensivo di audit trail. Senza ombra di dubbio questo ultimo dato serve solo a portare ulteriore confusione.

A questo punto ci viene quasi da chiederci cosa venga conservato con tanto zelo, se in realtà, per quanto emerso prima, ci pare che non ci sia niente che abbia le caratteristiche appropriate per essere conservato, a meno di volerlo utilizzare per qualunque motivo tranne scopi del tipo medico-legale, ma allora è davvero poco utile tutto il lavoro svolto fin'ora.



L'ultimo punto preso in esame è quello che riguarda le tipologie di Data Protection attivate. Come ormai è consuetudine, ci troviamo davanti ad una varietà di sistemi adottati che spaziano dagli strumenti dettati dalla normativa e per best practices, all'uso del dominio Microsoft che andrà via via mutandosi nel Single Sign-On di Oracle e ancora Active Directory, Antivirus, VPN SSL, politiche di archiviazione e back-up, l'autorizzazione tramite credenziali, la gestione dei livelli di autorizzazione degli utenti, la registrazione delle operazioni eseguite sul DataBase, e infine l'accesso ai sistemi che avviene tramite utente e password, i quali individuano i profili di autorizzazione. Anche in questo caso la fantasia ha portato i suoi frutti, fornendoci un numero di soluzioni ben maggiore rispetto il numero dei partecipanti al questionario, tanto più che raramente vediamo il ripetersi di una soluzione.



Da questa analisi emerge il fatto che ogni singola azienda si pone in modo differente dalle altre, pur facendo ognuna parte della stessa area vasta. Ognuna di esse ha implementato a modo proprio le varie funzionalità, il modo d'impiego, il raggio d'azione e il campo su cui operare, privilegiando ognuna un reparto o una specialità piuttosto che un'altra, ascoltando solamente le proprie necessità e, almeno apparentemente, mettendo in secondo piano l'ideale di seguire una linea comune a tutti.

Questo certamente non supporta qualsiasi idea di standardizzazione, molto utile se non indispensabile, ai fini di qualunque progetto che preveda, ad esempio, uno scambio dati, oppure un disegno in cui i documenti in oggetto oggi possano essere la base di qualche altro lavoro da considerare nel futuro.

Quello che possiamo affermare con certezza è che non possiamo si possa chiaramente mantenere la stessa linea guida per tutte le ULSS coinvolte, nel senso che andrà ideato un piano di lavoro differenziato per ognuna, tenendo presente le singole esigenze e ciò che di buono fosse già presente e attivo. Per tutto ciò che manca e che occorre ancora installare, si valuterà e studierà in una fase successiva cosa sia meglio per ognuna, adattando le necessità alle esigenze.

Come punto fermo rimarranno i passi assolutamente necessari da eseguire affinché il processo di dematerializzazione sia svolto a dovere, e quindi che la firma, l'archiviazione e la conservazione sostitutiva vengano sviluppate nel corretto modo.

9. BIBLIOGRAFIA e RIFERIMENTI in RETE

www.cnipa.gov.it

CNIPA, Decreto legislativo 7 marzo 2005, n.82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93 *Codice dell'amministrazione digitale* aggiornato dal D.Lgs. n. 159 del 4 aprile 2006 pubblicato in G.U. del 29 aprile 2006, n. 99 – S.O. n.105, *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale*, I quaderni di CNIPA, n.13, 2006

Deliberazione CNIPA 19 febbraio 2004, n.11, *Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti originali* –art. 6. Commi 1 e 2, del T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. (G.U. 9 marzo 2004, n. 57)

Decreto legislativo 22 gennaio 2004, n.42, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137*, G.U. 24 febbraio 2004, n.45 – Supplemento ordinario n.28

Decreto del Presidente della Repubblica 28 dicembre 200, n.445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (Testo A)*, G.U. 20 febbraio 2001, n.42 – Supplemento Ordinario n.30

Protocollo d'intesa tra il ministro per la pubblica amministrazione e il consiglio nazionale delle ricerche per la realizzazione di un programma di interventi per l'innovazione nel settore della salute, del 19 marzo 2009.

Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione, *Proposta di regole tecniche in materia di formazione e conservazione di documenti informatici*, 2008

CNIPA, *Evoluzione della normativa generale su documentazione amministrativa, archivi, protocollo (1990 – 2005)*, direttamente da www.cnipa.gov.it.

CNIPA, *Linee strategiche volte ad indirizzare le amministrazioni nella predisposizione del piano triennale per l'ICT 2010-2012*, adunanza del 24 settembre 2009

CNIPA, *Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML*, allegato alla deliberazione n. 34/2006

CNIPA, *Guida alla firma digitale*, versione 1.3, aprile 2009

CNIPA, *La dematerializzazione della documentazione amministrativa*, I quaderni CNIPA, n.24, aprile 2006

Ministro per l'innovazione tecnologica "*la dematerilizzazione della documentazione amministrativa – Libro bianco del Gruppo di Lavoro interministeriale per la de materializzazione della documentazione tramite supporto digitale*", marzo 2006 CNIPA

Pastura M. G., *Codice dell'amministrazione digitale: problemi e prospettive archivistiche*, I quaderni del CNIPA, n.25, maggio 2006

Ridolfi P., *Dematerializzazione dei documenti: idee per un percorso*, I quaderno di CNIPA, n.25, maggio 2006

Cleveland Cutker J., Ruth M., *Indicators of Dematerialization and the Materials Intensity of Use*, Center for Energy and Environmental Studies and Department of Geography, Boston University, USA, 1998

Corsi M., Gullo E., Gumina A., *L'impatto delle tecnologie dell'informazione sul settore delle Amministrazioni Pubbliche*, Estratti di Economia italiana, n.2, 2002

Bonfiglio Dosio G., *Primi passi nel mondo degli archivi. Temi e testi per la formazione archivistica di primo livello*, Cleup, 2003

Cammarata M., Maccarone E., *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Giuffrè, 2003

Cammarata M., *Firme elettroniche – Problemi normativi del documento informatico*, Monti&Ambrosini, 2005

Carucci P., *Lo scarto come elemento qualificante delle fonti per la storiografia*, Rassegna degli Archivi di Stato, XXXV/1-2-3, 1975

Ridolfi P., *Firma elettronica: tecniche, norme, applicazioni*, Franco Angeli, 2003

Massella Ducci Teri E., *Conservazione alternativa dei documenti*, I quaderni di CNIPA, n.37, luglio 2008

Fuga D., *Archiviazione Documentale e Conservazione Sostitutiva – Opportunità e vantaggi della dematerializzazione*, iged.it, anno XVI, n.3, 2007

Lisi A., *Responsabile del trattamento e responsabile della conservazione digitale: superare le criticità*, e-Health Care, Anno 1, No. 2, 2009

Massella Ducci Teri E., *Dematerializzazione della documentazione amministrativa*, iged.it, anno XV, n.2, 2006

Assocertificatori, Linee guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei titolari dei certificati di firma elettronica, versione 2.0, 2006

Castellani L., *L'interoperabilità dei protocolli informatici*, ForumPA, maggio 2009

HL7 XML Technical Committee, PRA level 1 specification, disponibile sul sito http://www.hl7.org/

Health Level 7 (HL7) Documentazione. Disponibile sul sito http://www.hl7.org/

www.firma.infocert.it/

Merighi F., *La firma digitale e le sue applicazioni*, disponibile sul sito www.cineca.it

Menezes A. J., Van Oorschot, Vanstone S. A., *Handbook of applied cryptography*, CRC Pres, 1997

Windley P. J., *Digital Identity*, O'Really Media, 2005

Adobe, Documentazione varia sull'argomento della firma digitale di tipo PDF, disponibile sul sito www.adobe.com/it/security/italiandigsig.html

W3C, *XML Signature Syntax and Processing (Second Edition)*, disponibile sul sito www.w3.org

Oasis, *XML Digital Signature profile of XACML v2.0*, febbraio, 2005, disponibile sul sito www.oasis-open.org

Verisign, Documentazione su Sicurezza e Certificati SSL, disponibile sul sito www.verisign.it

Verisign, (Documento Tecnico) *Unified Authentication di Verisign® La nuova generazione dell'autenticazione forte*, disponibile sul sito www.verisign.it

Palmirani M., *Sicurezza delle reti e dei sistemi informativi: accenni, Università di Bologna, Corso di Informatica Giuridica di base*, a.a. 2003/2004, I semestre

Rei C., *Protezione e meccanismi di non ripudiabilità del dato sanitario*, giornale

Bardavid E., *Conservazione sostitutiva. Normativa e consigli per realizzarla in modo semplice e sicuro*, SAN, 2007

Rossi Mori A., *Introduzione al progetto sui Livelli di Innovazione tecnologica In sanità – LITIS*, ForumPA 2009

Mangia M., *Il modello elaborato dal gruppo di lavoro sui Livelli di Innovazione Tecnologica In Sanità (LITIS)*, ForumPA 2009

Ramelli A., *Tutto il sapere sulla Dematerializzazione: dalla A alla Z*, Elzeviro, Treviso, 2009

Schael, T., *Workflow Management Systems for Process Organisations, Lecture Notes in Computer Science*, Vol. 1096, Springer, Berlin/Heidelberg

Lo Guzzo A., Schael T., *Outsourcing del ciclo attivo – la nuova sfida delle imprese per ottimizzare i processi con un partner esterno*, VoiceComNews, n. 4, ottobre-dicembre 2005: 48-51

D'Ignazio Serafino, *Product Manager Gestione documentale e Conservazione sostitutiva di InfoCert. La dematerializzazione in sanità*

Aymard M., Morelli M., Le carte della memoria: archivi e nuove tecnologie, Laterza, 1997

Mangia M., *Integrazione e cooperazione applicativa tra i sistemi informativi della sanità*

Trucco Paolo, Gastaldi Luca, *I Sistemi ICT per la clinical Governance: come uscire dalla fase di sperimentazione,* Politecnico di Milano, 2007

IBM Redbooks, *Single Sign-On Solutions for IBM FileNet*, Vervante, 2009

Yacono P. D., *Single sign-on influencing password security and usability in information systems*, Monash University, 2006

Nirmalan Sathianathan B., *A single sign-on protocol for fingerprint recognition systems*, California State University, 2004

Preite G., *Il riconoscimento biometrico, Sicurezza VS Privacy*, UNI Service, 2007

Rossano l., *Il processo produttivo – Schemi ed automatismi di un modello digestione e controllo per il miglioramento della qualità e il contenimento dei costi*, Francoangeli, 2001

Languasco A., Zaccagnini A., Introduzione alla crittografia, Hoepli informatica, 2004

Dimopoulos G., *Paperless Business & Lifestyle design with information & communication technology*, Digital Life Artist Inc

Ricciardi A., L'outsourcing strategico – Modalità operative, tecniche di controllo ed effetti sugli equilibri di gestione, Università degli studi della Calabria, Francoangeli, 2000

Hirschheim R. Heinzl A., Dibbern J., *Information System Outsourcing – Enduring Themes, new perspectives and global changes*, Springer, 2006

Wood M., Unix System Lab, *Audit trail administration*, Pentice Hall, 1992

InfoCert, *I documenti digitali e la conservazione sostitutiva: guida pratica per le imprese*, Il sole 24 Ore, 2008

Buccoliero Luca, Greta Nasi, Claudio Caccia, *e-Health: Percorsi di implementazione dei sistemi informativi in sanità*, 2005 McGraw Hill

10. RINGRAZIAMENTI

I miei ringraziamenti cominciano prima di tutto con un sentito "Grazie!" verso tutti coloro i quali, in questi anni, non hanno creduto in me: ebbene, signore e signori, sono arrivata alla fine, la palla torna al centro, ma il punto è mio.

Ringrazio i miei genitori, che mi han dato la possibilità di studiare, e anche per non aver mai creduto che avrei davvero lavorato come ingegnere.

Ringrazio i miei zii, Diana e Silvano, e mio cugino Luca, che han aspettato con ansia questo giorno, almeno per potermi finalmente cantare "Dottore, dottore, dottore del b*$o…..".

I nonni materni che a modo loro mi vegliano…

Alessandra, che ha sempre creduto in me e mi ha sempre spronato ad andare avanti, nonostante tutto, nonostante tutti: sei preziosa, e son 30 anni che me lo dimostri.

Un *grazie* particolare a Igor, che ormai mi sopporta e supporta, anche lui, da parecchio: ti dico solo… per fortuna che ci sei tu!

I miei "suoceri" Graziella e Cav. Lello che han gioito con me per gli ultimi esami e per il sospirato annuncio di laurea.

Le persone che mi han dato l'opportunità di laurearmi, mi hanno aiutato e molto mi hanno insegnato.

I miei compagni di corso, in primis Claudio, compare di tante sventure, di tanti esami (memorabile elettronica digitale!!), di tante vicende personali.

A seguire tutti, tutti gli altri compagni di corso, in accurato ordine sparso tra cui i ragazzi dei primi anni (Adriano, Giorgio "Tocio", Giorgio "Gighen", Martino), e poi tutta la banda del DEI, con Daniel, il Franz, Lord Henry, Annamaria (la Bionda), Francesca (la finta bionda), Mario (da Piva… ah no, Riva!), Alessandro, Simone "Castei", Alessandro "Mestrin", Alberto "Birra", Alberto Frenner, Bing, Carmen, Ivan, Francesco "Ciccio", Sheila&Denis, Giuseppe, Ilario, Lia, Marc'Aurelio, Maurizio PhD, Alfredo PhD, Omar, Paolo "Pol", Gemma, Filippo, Ivan "Ebay" (mio mentore!).

Amici vari sparsi qua e là, che si son dimostrati davvero preziosi: Livia (perché se non ci fossi stata tu, chissà se io&Ale saremmo potute uscire), Ale "Vela" (avanzo ancora le lezioni di vela, eh!), i vari compari dei corsi di danza e salsa come Carlo, Mara, Daniele, Nicola, Cedric, Alessia&Luca, Isabel, i compari "di concerti" Giuliano&Marina&Cinzia (perché per me siete una cosa sola), Elena "la francese", Hermina&Kevin (California, New Zealand, Padova, Paris, Kobe, New York City, Bruxelles.. prossima meta?), Nadia, Richard (Cow Boy, please remember me for my funny Tee), Shanny (Jaleo!!), Elvira, Michela (mi tocca laurearmi per riuscire a vederci), tutti il mio orgoglio padovano come Agostino, Max, Patrick, Simone, Fabio, Beba, Laura, Marco, Federico… ("come join the party, it's a Celebration"), ancora Silvia&Davide (Londra? Parigi? Berlino!), Diego (Tour 2011?), Sergio (dai che dobbiamo andar a far attraversare la strada ai rospi..), Arianna (capodanno, dove?), Alessio&Luca (semplicemente perché siete. punto.) …

Colleghi conosciuti in una lunga e movimentata carriera un po' dappertutto: Silvia (con cui ho diviso tante promozioni, e spartito parecchi omaggi!), Debora, Mattia, Roberto (MediaWorld), Sandra, Vanda e Enrico (Interspar), Max&Franz (HO), la squadra di Arsenàl, in particolare Luca e Andrea.

Le mie "alunne" delle ripetizioni che tanto mi han dato (leggi $$$..., anzi €€€).

Ryanair che mi permette di viaggiare in tutta Europa spendendo meno che una colazione al bar.

E ora un bel "*F*ck off, Mother F*ckers*": è stato indetto uno speciale trenino con posti illimitati con destino VFC (non è il codice IATA di un nuovo aeroporto, occhio eh..). A bordo c'è spaZio per tutti, ma i primi a salire e ad accomodarsi saranno a tutti quelli che mi han reso la vita difficile.

A tutte queste persone dico che, comunque, il loro pessimo atteggiamento ha solamente contribuito a rendermi più forte e a farmi diventare la carogna che sono oggi: sono qui, sono in piedi, alla fine del cammino, con le ossa rotte, ma ora perfettamente aggiustate e più sane di prima. Ho imparato a non mollare l'osso, a farmi valere, e comunque vada non mi fermo mai, mi spezzo ma non mi piego.

"This is who I am, You can like it or not,
You can love me or leave me,
'cause I'm never gonna stop, no no"

Si accalcano sulla piattaforma per poter salire sul treno anche tutte le anime maledette che mi han messo i bastoni fra le ruote, chi mi ha fatto cadere, chi mi ha dato dispiaceri, chi mi ha fatto arrabbiare, chi mi ha messo il morale a terra, che ha maltrattato i miei sentimenti, chi mi ha fatto passare le pene dell'inferno, amici vari (ma è più opportuno chiamarli nemici) che mi han reso difficile il cammino, gli invidiosi, gli ignoranti, le persone superficiali, i maschi che ti valutano solo in funzione della misura del tuo décolleté, coloro che non san gioire di ciò che hanno, quelli che ti considerano solo se indossi abiti griffati, "…*as for the cowardly, the faithless, the polluted - As for the murderers, fornicators, sorcerers, idolators, and all liars. Their lot shall be in the lake that burns with fire"and all murderers, fornicators, sorcerers, idolaters, and all liars … (Revelation 21:8 - Apocalypse)*".

Continuiamo con la padrona di casa che è da ottobre che non accende il riscaldamento anche se io lo pago, le ferrovie dello stato che vigliacche se i treni dei pendolari son in orario, Fastweb che abbassa la banda, le Poste che mi han lasciato 2 mesi a mezzo senza bancomat a Natale, Mastercard che nello stesso periodo ha deciso di sostituirmi la carta, Visa Electron che negli USA non funziona.

Le strade di Malta che sono una buca continua, e quelle di Tunisi che non son da meno, la Hertz che non ci vuole più come clienti, NYC che mi ha fatto contrarre la newyorkite, e Parigi che crea dipendenza comunque, Londra che non riesco proprio ad apprezzarla, le Canarie con le loro influenze intestinali, i cammelli o dromedari del Mar Rosso che salirci e scenderci è un impresa, Lubljana perché ogni volta sfuma l'occasione per andarci, Bruxelles che mi ha fatto pericolosamente scoprire la Kriek Cerise e Berlino la Berliner Weisse mit grun, Rodi perché un afa del genere non me l'aspettavo, la California che mi ha dato assuefazione da House of Pancakes, Barcellona perché un mercato della frutta così qui ce lo sogniamo, l'Irlanda perché 4°C ad agosto proprio no!, Stonehenge perché non si può più entrare all'interno del cerchio, Stratford-upon-Avon perché chiude alle 16 chiude già tutto, la Pink Lady in Costa Azzurra perché posti così sporchi non ne avevo mai visti, il Malawi perché ultimamente fa sempre la sua figura, la Sacher Torte di Vienna perché quando hai l'intolleranza al cacao non è un bel vedere, Venezia perché è l'unico posto dove proprio non riesco a orientarmi, Rogner-Bad che vigliacchi loro se mettono le segnalazioni, Stoccolma perché salta anche questa per malaugurate cause di forza maggiore, il bar/pasticceria/ristorante/libreria/centro culturale di Palermo di cui non so più il nome né l'indirizzo ma devo trovarlo, Sorrento perché solo lì la pizza ha ragione di esistere.

In coda anche Steven Klein che se fa un altro libro stavolta mi tocca accendere un mutuo, Frey Wille che non sbaglia una collezione (mannaggia!), Hurdertwasser che costruisce dal nulla e in the middle of nowhere una torre postuma e io ci sciropperemo 1200km giusto per vederla e tornare indietro, Dolce&Gabbana perché perdo i sensi e sbavo di fronte ad ogni loro vetrina, cacao/caffè/pomodori che mi ha dato l'intolleranza alimentare per 2 lunghissimi anni, LaCiccone perché sarebbe tempo e ora che tornasse a far un album decente, Vodafone perché con quei punti non riesco mai a raggiunger un premio, Starbucks che non si decide ad aprire in Italia, i signori Christian Louboutin-Manolo Blahnik-Jimmy Choo e le loro magnifiche scarpe,….

e poi visto che son in giornata buona, lascio a ognuno dei lettori 2 biglietti del treno (destino VFC, repetita juvant) da regalare a chi preferite!

- Fine documento -