Legislazione e Sicurezza nelle Telecomunicazioni e nelle Trasmissioni via Rete

Alberto Tibaldi

16 ottobre 2010

Indice

Capitolo 1

Lezione 01 : 04/05/09

1.1 Introduzione alla lezione

La legge fondamentale che "detta le regola" per la materia "privacy", nonchè per buona parte della trattazione, sarà il codice sulla privacy, ossia la legge 196 del 2003. Al fine di permettere ai cittadini la possibilità di "aggiornare" le proprie strutture e i propri mezzi per la nuova normativa, nonostante questa legge sia stata approvata il 30 giugno del 2003, essa è entrata in vigore solo dal 01 gennaio 2004. Questa legge è piuttosto stringente, dunque i sei mesi "tecnici" erano assolutamente fondamentali, al fine di poter preparare ogni macchina alla legge.

Questa legge sostituisce la precedente legge in materia di trattamento dei dati, ossia la 675 del 1996: essa venne promulgata il 31 dicembre dell'anno 1996 ed entrata in vigore (per gli stessi motivi) nel maggio del 1997, a causa di una normativa europea del 1995 (95/46/CE): essa fu la prima normativa in ambito di trattazione dei dati in Europa, e tra le prime in ambito mondiale.

Gli enti che principalmente interesseranno questa trattazione sono i seguenti:

- III corte di cassazione: si tratta della corte che dirime le questioni informatiche;
- CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione): si tratta di un organo legislativo e operativo, che può fare ispezioni assieme alla GDF (Guardia Di Finanza), alla Polizia Postale, all'Interpol e ad altri enti.

Buona parte della trattazione, in diverse lezioni, presenterà il codice sulla privacy, evidenziandone diversi aspetti.

1.2 Legge 196/2003 : Codice sulla Privacy

La materia "privacy" riguarda fondamentalmente una cosa: la trattazione delle informazioni personali.

Le informazioni personali possono o meno essere comunicate: a seconda delle informazioni, e del contesto in cui ci si trova, si può avere o meno il diritto di non comunicare alcune informazioni, a seconda della loro importanza.

Nome, cognome, indirizzo sono in elenchi pubblici, dunque informazioni pubbliche, che devono essere comunicate: l'identificazione di una persona è assolutamente obbligatoria e inevitabile. Ciò non significa tuttavia che queste informazioni possano essere utilizzate in maniera assolutamente libera; un esempio classico in cui spesso si infrange il codice è l'annuario del liceo: quando si introducono le foto di classe nell'annuario di un liceo, bisogna chiedere se si desidera comparire nell'elenco: associare a una foto nome e cognome si può fare, solo in seguito ad un'autorizzazione scritta e firmata. Alternativa sarebbe quella di utilizzare dei nickname, ossia degli pseudonimi dell'individuo. L'autorizzazione ovviamente deve esistere per ogni singola persona e su di ogni singolo dato.

I dati che riguardano la persona possono dividersi in tre fondamentali categorie:

- Dati generali;
- Dati semisensibili;
- Dati sensibili.

Esemplificazioni dei vari dati verranno presentate lungo tutto il corso della trattazione; per ora si può dire che i dati generali sono i dati che figurano in elenchi ufficiali, e devono essere resi pubblici. Essi derivano dall'istituzione dai quali vengono gestiti (generalmente, l'anagrafe). Nome, cognome, indirizzo, sono alcuni di questi dati, e si possono vedere nell'ufficio dell'anagrafe della città interessata. A seconda del contesto possono esistere diversi dati generali: al Politecnico ad esempio i dati generali sono nome, cognome, matricola, ossia i tre dati che permettono di identificare, nel contesto del Politecnico, un individuo, una persona fisica. Esistono elenchi pubblici in cui si può associare il nome e il cognome di un individuo a una matricola, che dunque identifica in maniera univoca ciascun individuo all'interno del Politecnico. Gli altri dati sono gestiti dal Politecnico, in modo da non intaccare le caratteristiche della privacy della persona.

Ci si pone una domanda di esempio: quando si vedono istituzioni particolari come una ASL, al momento del ritiro degli esami del sangue per esempio, come si dovrebbero "chiamare", in pubblico, gli interessati? Beh, le possibilità sono diverse: nome, cognome, codice fiscale, numero di tessera sanitaria, altro. La risposta giusta è "altro": dal momento che i dati sanitari di una persona sono sensibili, ossia estremamente riservati e delicati da trattare, le persone devono essere convocate mediante un "codice", assegnato al momento del ritiro degli esami, che permetta di mantenere per quanto possibile la massima riservatezza sui dati sanitari dell'individuo in questione. Alcuni esempi di dati sensibili sono i seguenti:

- Dati sanitari (attuali o passate patologie, gruppo sanguigno..);
- Coordinate bancarie;
- Abitudini sessuali;
- Appartenenza a partiti politici;
- Provenienza etnica;
- Convinzioni religiose;
- Eventuali problematiche giuridiche.

I dati sensibili sono generalmente difficili da trattare in qualsiasi contesto; i dati generali variano a seconda del contesto in cui ci si trova: ci sono contesti in cui l'indirizzo è un dato non trattabile, altri in cui è un dato pubblico, e così via. Al Politecnico ad esempio nome e cognome sono dati pubblici, e anche l'associazione con la matricola lo è; gli altri in teoria non andrebbero trattati.

Considerando ancora il Politecnico, un momento importante è la consegna dei risultati, mediante tabelloni, per un esame. Nome e cognome sono dati pubblici, dunque farli figurare di fianco al voto non è contro la normativa sulla privacy. Si parla più che altro di "regole di buon gusto": sarebbe meglio se figurasse solo la matricola (a partire dalla quale si potrebbe comunque collegare nome e cognome), per quanto comunque non si infranga alcuna norma, se non il "buon gusto".

In una banca, il dato generale (comunicando tuttavia solo con gli impiegati) è il numero di conto corrente bancario. Questo dato non è tuttavia generale nel senso che ciascun utente della banca può conoscere le coordinate bancarie di ogni altro individuo: questo è un dato comunicabile solo agli impiegati/dirigenti competenti; al momento della comunicazione con l'impiegato,

è buona cosa che tutti i personaggi all'interno della banca non coinvolti con la relazione utente-banca siano lontani dall'utente, in modo da evitare di acquisire informazioni che non competono loro.

Ciascun contesto è separato a "compartimento stagni": non vi deve assolutamente essere la possibilità di ottenere, per ciascun individuo, informazioni che non riguardino il contesto. Supponendo ad esempio di fare un controllo sulla patente, in seguito ad un posto di blocco stradale la cui competenza è quella di controllare infrazioni al codice della strada, non è possibile e non deve essere possibile, a partire da essa ottenere informazioni sanitarie, bancarie, politiche dell'individuo: in ogni ambito di lavoro un operatore può esclusivamente vedere e trattare dati che lo interessano.

Esiste un anello di congiunzione tra tutti i vari ambiti: volendo pensare a ciascun contesto come a diversi compartimenti separati verticalmente, esiste una linea di congiunzione "orizzontale" in grado di unire tutti i vari ambiti; questa "linea trasversale" è il codice fiscale dell'individuo. Un codice fiscale viene associato a ciascuna persona qualche ora dopo la sua nascita; a Roma, nel quartiere Tiburtino, esiste un cervellone che, a partire dal codice fiscale, è in grado di tirar fuori qualsiasi informazione sull'individuo, di qualsiasi importanza e di qualsiasi tipo. Dal momento che il codice fiscale è un dato estremamente sensibile, nonchè estremamente potente, esso può essere usato in sede di giudizio esclusivamente in seguito all'autorizzazione di un magistrato.

1.3 Privacy e aziende

Finora si è parlato esclusivamente di persone fisiche; per persone fisiche, generalmente, si intendono gli esseri umani in quanto soggetti di diritto. Nell'ordinamento italiano sono persone fisiche gli esseri umani che con la loro nascita diventano soggetti rilevanti ai fini del diritto, in quanto secondo l'articolo 1 del codice civile divengono titolari di diritti e doveri, cioè acquisiscono la capacità giuridica.

Per quanto riguarda le attività di un qualsiasi tipo, si introduce un altro tipo di persona, ossia la cosiddetta "persona giuridica": si tratta di una persona "astratta", che però diventa concreta sotto il punto di vista della capacità giuridica in seguito all'associazione di una partita IVA. Associando un codice fiscale a una partita iva, si ottiene la definizione di persona giuridica. In sostanza si associa, a un complesso di persone e di beni, la capacità giuridica, rendendola dunque un soggetto di diritto.

Una delle operazioni effettuabili tra aziende è il trasferimento di capitali; nei tempi moderni, tutte queste operazioni vanno informatizzate, al fine di

essere ben documentate e controllate dagli enti appositi. Annualmente o più volte l'anno devono essere trasmesse a Roma le informazioni concernenti i capitali e non solo, riguardo un'azienda.

L'azienda comunica al più ogni anno, entro il 31 marzo, un insieme di caratteristiche dell'azienda, in un documento denominato DPS (Documento Programmatico sulla Sicurezza), nel quale si comunicano informazioni di vario genere. Questo documento va consegnato al ministero della finanza e a quello delle infrastrutture; esso deve contenere diverse informazioni, tra cui:

- Quante persone lavorano nell'ambito dell'area informatica;
- La responsabilità di ciascun individuo;
- Chi ha accesso alle reti telematiche, a quali reti, con quale titolo.

Con la precedente normativa (675/1996) l'amministratore delegato assegnava tutte le responsabilità della sicurezza dell'azienda a un singolo individuo, che avrebbe dovuto rispondere direttamente anche al ministero delle infrastrutture; la legge 196/2003 ha tagliato le responsabilità al vertice, all'amministratore delegato e all'individuo designato, in modo da distribuire in maniera più omogenea, a diversi individui, diverse responsabilità, evitando di colpire un'unica persona per colpe che magari non gli competevano neanche direttamente.

Per quanto riguarda le banche, i flussi al giorno d'oggi sono totalmente informatizzati, ossia viaggiano esclusivamente per reti telematiche. I flussi vengono pilotati verso le centrali, e partono in una sorta di "flowing" a fine giornata, quando nessuno è più presente in ufficio e gli impiegati hanno terminato il lavoro. Una volta addirittura i flussi, i trasferimenti, partivano esclusivamente il venerdì sera, al termine della settimana lavorativa.

Per avere sistemi estremamente sicuri si utilizzavano, un tempo, calcolatori estremamente sicuri, quali il "computer cray": si tratta di un calcolatore nato verso il 1988, costituito da più CPU che lavorano in parallelo. Con diverse unità le macchine diverse in posti diversi si mandano il calcolo e lo eseguono in parallelo. L'implementazione più "potente" è il Cray-2.

Capitolo 2

Lezione 02 : 11/05/09

2.1 Prosecuzione studio del Codice sulla Privacy

Come già detto, a partire dalla normativa europea 95/46/CE, si dovette elaborare una prima normativa locale per la privacy: la 675/96. In seguito alla nascita di un certo numero di elementi e problematiche, venne elaborata la 196/2003, attualmente in vigore. La nascita della 95/46/CE era dettata dalla necessità: nel 1995 internet si usava ancora poco, dal momento che il boom in Italia avvenne nel 1997/1998; negli Stati Uniti tuttavia internet aveva giò preso piede nel 1995, cosa che faceva intendere che presto in Europa sarebbe capitato lo stesso. Internet rappresentava una vera minaccia per la privacy delle persone, dal momento che si inviavano moltissimi dati, che risultavano essere pubblici a chiunque. Altra cosa molto insicura erano i protocolli per l'acquisto di merci.

Una forma di acquisto via rete (per quanto prevalentemente telefonica) riguardava la spesa ai supermercati: i supermercati davano ad esempio la possibilità di fare la spesa telefonando alla mattina, dando la lista della spesa, se i clienti in questione erano nell'elenco dei clienti con questo servizio abilitato. Sulla base dell'ammontare della spesa si guardava nelle capacità monetarie dell'utenza, si prelevava l'ammontare e si telefonava al cliente dicendo di andare in un parcheggio e prelevare il carrello della spesa, completando la transazione. Questo metodo di commercio elettronico presentava molti difetti:

- Si avevano troppi dati a disposizione dei supermercati: ciascun operatore poteva vedere quanti soldi aveva il cliente, cosa assolutamente insensata: bisogna verificare solo che si abbia la possibilità di pagare, non la disponibilità monetaria totale del cliente;

- Troppa libertà: si potevano prelevare soldi in modo sregolato, senza vincoli, rispetto alla richiesta;
- Era anche possibile che qualcuno rubasse il carrello al momento della consegna.

Le necessità erano, nel mondo, fondamentalmente due:

- Bisognava limitare il traffico di armi;
- Bisognava contemporaneamente liberalizzare le frontiere, facendo cadere i controlli sui documenti fisici (passaporti) e sulla circolazione di beni e persone.

In Europa si cercò di fare ciò mediante l'accordo di Schengen: le persone identificate mediante la carta di identità, di circolazione, potevano circolare senza dazi doganali o senza passare per agenti doganali. Ora l'Unione Europea ha 27 paesi, di cui 15 hanno sottoscritto il patto, 19 sono in fase di discussione. Gli unici controlli ammissibili riguardano la possibilità di contrabbando di merci o simili.

Nel 1995 l'UE cercò di incentivare il commercio elettronico, in modo da incentivare la nascita di nuovi posti di lavoro. Riguardo il commercio elettronico, dunque, l'UE emanò alcune linee guida che costrinsero i paesi ad essa appartenenti a legiferare, ossia ad emettere diritto in un certo senso.

Come è ben noto, la legislazione va molto più lentamente della tecnica, della tecnologia: come già detto, la 196/2003 venne approvata nel giugno del 2003, ma entrava in vigore solo sei mesi dopo, in modo da dare il tempo di "prendere atto" a tutti gli organi. L'Unione Europea propose solo linee guida; i 27 paesi dell'UE la pensano di fatto in 27 modi diversi, dunque, aldilà di queste linee guida, ognuno fece a modo proprio. Si cerca di armonizzare la legislazione, e c'è stato un tentativo di avvicinare paesi distanti. In tal direzione, Italia, Germania, Belgio vanno abbastanza bene.

Nell'ambito della comunità europea la legge sulle reti dovrebbe essere uguale: bisogna specificare, per i diversi ambiti, quale diritto vale nel caso un abitante di una nazione si trovi in un'altra (ad esempio, un italiano in Francia). Dal 1995 a oggi sono passati ben 14 anni, e vi è una certa chiarezza nelle leggi: il cittadino di una nazione, in una nazione diversa dalla stessa, se è lì per turismo risponde di solito alla normativa della propria nazione, a meno che non abbia effettuato un reato palese; se invece vende servizi, deve per forza applicare il diritto e la legge della nazione in cui si trova fisicamente.

Nel commercio elettronico, virtuale, quale diritto si deve applicare? Il diritto che vige di solito è quello dell'utente: se l'utente dimostra di essere

stato buggerato dal venditore dell'altra nazione, quello che si fa di solito è far intervenire il foro nel quale si trova l'utente, per far svolgere la contesa giudiziaria. Nel caso di banche, assicurazioni o simili, in realtà sono le medesime a scegliere quale sia il foro nel quale portare la controversia: in questo caso vince il venditore, e non l'utente, a causa dello strapotere di organizzazioni di questo tipo.

Tutte queste sono le necessità che hanno portato l'unione europea a emettere linee guida sia sul commercio elettronico sia sull'ambito della privacy.

L'Italia non aveva mai regolato nella Costituzione nulla riguardo la privacy: la 196/2003 è infatti fuori dall'ambito costituzionale, dal momento che si aggancia soprattutto al codice civile, ossia al codice che contiene i possibili comportamenti di persone fisiche o giuridiche in modo che rispondano alle leggi. Per quanto riguarda la privacy, la circolare applicativa è stata emessa, dunque è in vigore.

Nazioni come Spagna e Portogallo hanno introdotto norme sulla privacy a livello costituzionale, anche se si tratta di un caso piuttosto isolato; in Inghilterra la situazione è invece differente rispetto agli altri paesi, dal momento che le leggi in parte sono scritte, ma per la maggior parte orali (ossia si basano su sentenze emesse): parte del corpus giuridico è esclusivamente fondata su sentenze rpecedentemetne esposte, cosa che in Italia non sarebbe possibile. Tutta la normativa per la Privacy è nella 196/2003, mentre i documenti aggiuntivi devono essere emessi (quale ad esempio il DPS).

2.2 Prosecuzione studio Privacy e Aziende

Riparlando del DPS, la sua definizione è introdotta nella 196/2003, come anche i contenuti che deve avere al fine di essere valido: si devono avere precise informazioni sulla sicurezza, sull'organigramma dell'azienda, sul layout delle macchine depositarie delle informazioni, sulla mappatura delle reti fisiche, specificando informaszioni riguardo:

- Macchinari;
- Software;
- Persone.

Supponendo di parlare di un'azienda di telecomunicazioni, vi sarà un responsabile capo, che nel suo ambito avrà anche responsabilità di referente riguardo il codice sulla privacy. In Italia, con la 196/2003, l'amministratore delegato nomina un ISSO, il quale stabilità a sua volta un organigramma

per livelli, ottenendo dunque organizzazioni su piani orizzontali e verticali. Ciascun operatore usa una certa macchina o un certo login e password, e, possibilmente, una smart card (specie se si utilizzano dispositivi esterni); la smart card deve restare nel computer per tutta la sessione di servizio, quindi si può estrarre se e solo se termina la sessione di lavoro, o in casi speciali. Se ad esempio l'operatore arriva al mattino sulla sua postazione di lavoro e deve introdurre dati riservati, si deve seguire la procedura di login.

I terminali (ossia le macchine destinate agli operatori) non devono essere spenti: vi devono essere procedure in batch che controllano le operazioni di login, le singole operazioni, difformità rispetto alle procedure, anomalie tecniche e quant'altro; una volta che si immettono login, password, smart card, la sessione viene aperta e ci sono le operazioni da leggere prima dell'immissione dei dati (alcune operazioni da fare). Se la macchina non funziona, o se per tre volte si sbaglia la password, ci si rivolge al responsabile per l'informatica e si chiederà se vi sono macchine libere. In tal caso il responsabile può (o meno) dargli l'autorizzazione, segnando che l'operatore quel giorno è collegato a quel computer, segnalandolo al centro servizi centrale di Roma. Informazioni di questo tipo, quali la trattazione di questi dati e di queste situazioni, la sicurezza informatica, il personale addetto e simili, vanno introdotti nel DPS. Altro elemento che si trova nel DPS, nonchè nella legge 626/94 (legge sulla sicurezza al lavoro), è la pausa ogni due ore: ogni due ore è obbligatorio effettuare una pausa di 15 minuti. Questo caso è interessante dal momento che, quando la persona si allontana, deve fare il logout, togliere la smart card e dunque andare in pausa. Vi sono dei contatori di servizio pattuiti nel contratto: nel caso si vogliano avere dei bonus lavorativi, essi permettono di verificare e quantificare la produttività delle persone.

Le macchine moderne impostate per il lavoro devono avere un certo hardware, essere tendenzialmente dei terminali, non dei desktop: per terminale si intendono macchine dotate di tastiera, mouse, lettore di smart card; non vi deve essere la possibilità di avere supporti rimovibili, quali floppy drive, masterizzatori, DVD players (dal momento che sarebbe possibile, mediante essi, da un lato prelevare dati importanti contenuti nella rete quali licenze, programmi o informazioni, dall'altro introdurre elementi negativi nella rete quali virus o simili). Le licenze dei programmi sono o monouso (ossia una per ciascun utente) o aziendali (ossia per un certo numero di macchine contenute nell'azienda).

Un modo di esportare informazioni dall'azienda è mediante l'uso di supporti rimovibili; un altro modo, ovviamente, è quello di effettuare stampe. Si parla in questo contesto di "stampe sicure": le stampe normali per essere fatte richiedono identificazione, mediante almeno smart card; le stampe sicure utilizzano stampanti con ID, in stanze chiuse a chiave. L'obiettivo di

tal sicurezza e tali identificazioni è quello di associare, per ciascuna stampa, un nominativo, in modo che chi effettua stampe si assuma la responsabilità di ciò che ha stampato.

Oltre all'informazione sull'hardware esiste un "codice deontologico", ossia un insieme di regole riguardo il comportamento dell'operatore all'interno di un qualsiasi luogo di lavoro, rispetto ai dati sensibili. L'operatore deve rispettare tutti i dati su persone fisiche e giuridiche, utilizzando solo quelli che lo competono.

Come già detto, per persona giuridica si intende l'ente che rappresenta un'azienda e/o un gruppo di persone; ad essa si associa una partita IVA e un codice fiscale di una persona fisica, su cui vi sono tutti i riferimenti all'azienda.

2.2.1 CRM

Per quanto riguarda la gestione dei clienti di una certa azienda o di un certo servizio, è stato creato (e implementato) il concetto di CRM (Customer Relationship Management): esso sostanzialmente è, in termini informatici, un programma che dà la possibilità di gestire dei dati, al fine di interfacciare l'utenza con l'azienda. Esso è un programma intelligente comulativo in grado di gestire dati in modi molteplici, e di effettuare un certo numero di operazioni. In un CRM sono contenuti word processors, fogli di calcolo, moduli di comunicazione con altri computer, database per la gestione di nominativi e relativi dati. Si ha all'interno del software una serie di puntatori intelligenti in grado di pescare su diversi database, collegandosi al sistema mediante reti interne o mediante altre vie. Ogni puntatore può essere uno dei dati della persona, ad esempio codice fiscale, cognome, targa dell'automobile, cartella clinica, numero di polizza assicurativa. L'ISSO, ossia il responsabile della sicurezza informatica e compilatore del DPS nominato dall'amministratore delegato, nel DPS dovrà specificare tutte le caratteristiche del CRM che si utilizza nell'azienda.

Per un CRM, ossia uno di questi mega-software contenenti tutti i tool necessari per la gestione e il lavoro, si hanno licenze utilizzabili dalle 2 alle 56000 persone; possono esserci release di aggiornamento (che andrebbero segnalate nel DPS quando effettuate). Generalmente, un CRM si installa in un unico computer, per poi condividere l'uso sulle varie macchine mediante rete. In ambito di CRM, si parla generalmente di reti chiuse, ossia non accessibili dall'esterno della struttura (si noti che la legge dice esplicitamente che queste reti non possono essere aperte): uno, due o n server gestiscono i programmi (quale il CRM), o parte di esso, lo condividono, tengono conto della memoria storica incrementale (incrementale dal momento che giorno per

giorno vengono effettuate mediante il programma sempre nuove operazioni, che vanno loggate). Chiudendo la rete si fa in modo da non comunicare con l'esterno, cosa che possono fare solo alcuni responsabili, ma utilizzando una rete diversa da quella di lavoro e in modo da non farla comunicare con quella interna (utilizzando anche macchine diverse, almeno una per rete per operatore).

Esistono alcune semi-eccezioni alle regole, per esempio in ambito sanitario: quando può essere necessario trasferire velocemente informazioni di tipo sanitario o clienti da un polo ad un altro (il polo sanitario di Torino è collegato con altri due o tre poli nel nord italia, dunque le cartelle cliniche per alcune patologie, nella fattispecie nel caso sia necessario effettuare operazioni di cardiochirurgia o neurochirurgia, possono essere trasferite senza problemi da un ospedale a un altro, previa autorizzazione del paziente o di chi ne fa le veci). Ogni trasferimento deve essere supervisionato, sia in trasmissione sia in ricezione, dal responsabile locale della privacy, a meno di casi di estrema emergenza (quale ad esempio il caso Thyssen, dove la salute prevale sulla legge, dunque si può evitare lo studio delle autorizzazioni al fine di usare tutti i mezzi per salvare la vita dei feriti).

Tutto ciò come si è capito dipende dai responsabili della privacy, ma dunque è regolamentato dalla legge 196/2003: essa dice come trattare i dati riservati, ma anche (mediante allegati, quali il ben noto DPS) come vanno trattati al fine di non ledere i diritti dell'utente. Con dati generali i danni sono inferiori, rispetto a quelli provocabili mediante il cattivo trattamento dei dati sensibili. Di tutti i possibili dati, i due più gravi da trattare sono:

- Dati sanitari;
- Dati giudiziari.

Nel primo, la responsabilità è di chi trasmette e di chi riceve i dati; nel secondo caso, quello dei dati giudiziari, al fine di effettuare trasmissione o ricezione di dati è necessario avere il permesso di un magistrato, dunque la trattazione è estremamente complicata: l'unico che autorizza l'apertura dei casellari per reati civili e/o penali è un magistrato (questo, in Italia e generalmente in Europa).

18 nazioni hanno sottoscritto l'accordo nazionale seguendo le linee guida; essi possono comunicarsi tra loro dati su reati civili e/o penali, quindi tutto è possibile, sempre a patto che vi sia un magistrato che permetta le transizioni internazionali. le nove nazioni mancanti sono sotto osservazione: solo quando avranno implementato protocolli informatici sicuri e tali da permettere senza rischi il trasferimento di dati giudiziari, potranno fare parte a tutti gli effetti della UE sotto anche questo punto di vista.

Capitolo 3

Lezione 03 : 18/05/09

In questa lezione si tratteranno sostanzialmente due argomenti: digital divide, e commercio elettronico.

3.1 Digital Divide

3.1.1 Telefonia

Una delle grosse problematiche che interessano la legislazione informatica moderna è il digital divide, "gap digitale", "scarto digitale", tra qualcuno che ha una certa disponibilità tecnologia, di mezzi digitali, e altri che non ne hanno, per varie motivazioni (tecniche, personali, economiche). Uno dei casi più interessati è quello delle tecnologie "wireless", e la telefonia non tanto fissa, quanto mobile. Per quanto riguarda la telefonia fissa, il 97 % delle aree geografiche italiane sono ricoperte, mentre il 3 % è sostanzialmente costituito da zone montuose e disperse o molto elevate, in cui il prezzo sarebbe troppo elevato per l'utenza: il gestore in tali zone lavorava e pagava fino a un certo punto, oltre l'utenza, rendendo i prezzi inaccettabili.

Anche nel caso della telefonia mobile si ha una copertura del 97 %, ma bisogna studiare la differenza tra i vari operatori: i quattro operatori grossi della telefonia mobile italiana hanno coperture diverse, che per 3 dei 4 operatori son sempre pari al 97 %; i territori non sono ricoperti in maniera omogenea. Il problema è sempre il solito: quello delle aree montane. Il quarto operatore ha una copertura circa pari al 78 %, dunque più limitata. Per legge, sia il canale della telefonia fissa sia quello della telefonia mobile deve essere occupato.

3.1.2 Accesso a internet mediante wireless

Per la tecnologia wireless il discorso è un po' diverso: non si ha un limite minimo di copertura imposto, dal momento che questa non può essere garantita in modo da soddisfare tutta l'utenza. Si è tentato un programma di copertura wireless in certe zone. Per quanto riguarda la sicurezza, sono caduti i vincoli della protezione: si filtrano alcune possibilità e alcuni canali per proteggere almeno le persone, garantendo comunque un accesso libero. Un esempio è quello dei comuni in cui sperimentalmente sono state introdotte reti wireless libere per gli utenti, ovviamente con alcune restrizioni.

3.1.3 Digital divide e mafia

Una forma di digital divide, per quanto meno considerata, può essere quello tra forze dell'ordine e delinquenza: i delinquenti di una certa portata (quali le associazioni a delinquere, le "mafie"), hanno a disposizione una grossa capacità monetaria, ma dunque hanno a disposizione strumentazioni molto sofisticate, anche più delle forze d'ordine. Si ha ad esempio a che fare con navi con schermature anti-radar, e anti-filtraggio di segnali, in grado di non far captare i propri segnali alla polizia.

3.1.4 Pedopornografia, sanità e altre necessità

Verranno a questo punto presentati alcuni esempi specifici in cui si è parlato del problema del digital divide, nonchè del potere delle autorità rispetto ad alcuni abusi nella rete.

Ciò che spesso si fa in qualche modo è utilizzare dei prestanome, volontari o meno. Un caso molto noto di pedopornografia riguarda quello di un computer pescato a visitare insistentemente siti pedopornografici nel Pacifico; il numero di telefono associato alle suddette visite era registrato a nome di un anziano signore, 98enne, dunque sicuramente o quasi non colpevole. Un'indagine durata due anni ha permesso di scoprire il fatto che vi fosse un nipote furbo, che aveva fatto comprare un computer al nonno, per sfruttarlo in modo da discolparsi. Le indagini tuttavia non sono semplicissime da fare: solo una volta trovata la quasi-certezza del colpevole, o quantomeno isolate 3-4 persone tra cui vi siano i colpevoli, si può uscire allo scoperto.

Un caso in cui si è dovuta utilizzare una digitalizzazione, provocando un gap rispetto ad altre nazioni, è la sanità islandese: l'Islanda è l'unico paese al mondo in cui sia stato effettuato un processo di totale informatizzazione dei dati sanitari. Trattandosi di un territorio poco popolato, in cui sono presenti patologie strane, causate dall'isolamento della popolazione e dai climi rigi-

di, dall'alimentazione, si è deciso per il bene della popolazione di sacrificare parte della privacy delle persone, rendendo noti gruppi sanguigni, caratteristiche linfatiche ed ematologiche. Vi è tuttavia un'autorità, un garante per la protezione dei dati personali e sanitari, che visita con alcuni tecnici le strutture in modo da verificare che i dati vengano trattati nella maniera corretta, rendendo impossibile la circolazione di dati non dovuti se non in presenza di rischi notevoli per la popolazione. Si noti che l'Islanda appartiene all'EFTA, ossia un'organizzazione commerciale (non politica/economica come l'UE), cui appartengono altri paesi come la Norvegia; tra i paesi dell'EFTA è possibile esclusivamente una facilitazione delle transizioni di beni o servizi, assolutamente non di qualsiasi altra informazione, quale questo enorme database sanitario.

In Italia per quanto riguarda patologie particolari quale ad esempio il virus H1N1 (febbre suina) la legge sulla privacy può venire meno (come peraltro nel già citato caso Thyssen): quando una persona arriva in Italia, ad esempio a Malpensa, e si scopre che proviene da Città del Messico, è necessario assolutamente trattenerla, indipendentemente dai diritti della privacy: essa può infatti non dichiarare, in buona fede o meno, il fatto di essere infetta. Si deve limitare il traffico a costo di danneggiare le persone sotto il punto di vista della privacy per monitorare le persone, almeno per il possibile periodo di incubazione della malattia.

Altro caso in cui la privacy può venire meno, e si cerca di colmare il digital divide, è il caso delle calamità naturali: quando vi fu Katherine a New Orleans, essa venne quasi distrutta, e le autorità di sicurezza (quali la Farnesina) autorizzarono le società a inviare un messaggio a chi era lì, ledendo il diritto alla privacy ma aggiungendo possibilità di salvare vite o ottenere informazioni. Usi impropri dei numeri di cellulare o altro, quali segnalazioni di eventi non vitali o ancor peggio per scopo di lucro (pubblicità), sono assolutamente punibili per il codice sulla privacy.

3.2 Commercio Elettronico

Per quanto riguarda il già nominato commercio elettronico, come già accennato in precedenza l'Unione Europea ha fatto molta leva, al fine di propagarlo; le varie nazioni, tuttavia, hanno piazzato dei paletti ben definiti per la sua applicazione. Il commercio elettronico passa per canali "web-sites". Per questo si deve rispondere a regole diverse rispetto a quelle del commercio tradizionale: per un negozio elettronico è necessario effettuare operazioni di installazione e vendita su web, sia di prodotti sia di servizi; l'idea, tuttavia, è

fondamentalmente quella di associare il commercio elettronico al tradizionale negozio in cui si compra.

I negozi elettronici devono rispondere sulla sicurezza e sulla certezza del prodotto venduto; raramente un venditore vende a nome diretto, ossia vende direttamente sul web, dal momento che si appoggia a qualcun altro, che mette a disposizione la canalizzazione del flusso. eBay ad esempio mette a disposizione la tecnologia. Per motivi economici un tempo si veicolavano anche i canali di immissione delle informazioni; come cliente si può scegliere quale piattaforma utilizzare, facendo in modo che, chi deve fornire il servizio, lo faccia al meglio per ciò che gli si paga.

Un provider generalmente affitta le linee alle varie piattaforme; ciò che si ha, dunque, è fondamentalmente una struttura composta da tre elementi:

- Provider;
- Piattaforma;
- Utente.

L'utente può essere un privato, un negozio; il proprietario di piattaforme mette sempre e solo a disposizione una struttura, il provider fornirà il canale, ed esso dovrà garantire un servizio. Il provider dovrà dunque comportarsi in maniera conforme rispetto alla legge.

Ciò che si fa in pratica è la seguente cosa: un venditore va da un provider; nella pagina del negozio elettronico il venditore dovrà essere sempre visibile agli acquirenti in maniera inconfondibile, con un certo insieme di informazioni: numeri di telefono, FAX, indirizzo di riferimento per una sede alla quale ritornare eventuali prodotti. Se il venditore vende, dovrà anche far figurare quale protocollo di sicurezza è stato implementato (informazioni fornite da piattaforma e provider). Solo il venditore (a meno di casi molto particolari) potrà vedere qual è la banca cui è affiliato l'acquirente, e verificare se la transazione economica è avvenuta (assolutamente non informazioni superiori, quali l'ammontare complessivo del conto corrente).

Il proprietario di piattaforma è quello che possiede "tutte le linee": questo può essere un gestore di telefonia fissa. Ciascun proprietario di piattaforma è provider, ma solo per i propri prodotti: apparecchiature e servizi di telefonia fissa, ma niente più. Il provider nel senso del commercio elettronico fa da mediatore tra la piattaforma e il venditore; spesso, tuttavia, esso sarà diverso dal venditore vero e proprio dell'oggetto.

Di solito, quando si ha un dolo, esso è o del provider o del venditore: il provider di fatto conosce molte, troppe informazioni, dunque la 196/2003 dice che anche solo chi fornisce software freeware, per esempio, deve rispondere al

fatto che coloro che lo scaricano si sono collegati da un certo posto e simili, una volta sottoscritto una dichiarazione di non commettere reati. Il provider, avendo a disposizione molte informazioni, deve loggarle e mantenerle per la legge. Ciò che si è preferito fare è separare le responsabilità; quali siano le regole in vigore tuttavia dipende dai vari paesi: USA, UE, Canada, Australia, ecc.

Per il negozio elettronico si hanno, generalmente, diverse condizioni, diversi requisiti, quali ad esempio un font size idoneo, in grado di essere letto; colori che non impastino il testo o lo rendano illeggibile, website in più pagine, uso del protocollo SSL3. Fondamentale è il ruolo del catalogo: esso è regolamentato ed è obbligatorio se chi crea il negozio elettronico vende una pluralità di prodotti. Deve essere in bella vista sul sito, in modo da renderlo facile da trovare e da leggere per l'utente. Non si hanno indicazioni da parte del legislatore su quanto ampia deve essere la pagina che descrive le caratteristiche del prodotto: i dati potrebbero non essere esaustivi, e la legge lo permette.

Un caso un po' particolare di commercio elettronico riguarda due tipi di prodotti: vestiti e automobili. In teoria essi possono essere venduti, ma, dal momento che non è possibile verificare il colore e le caratteristiche del tessuto, la consistenza, il rischio è dell'utente: l'utente non ha la minima garanzia di poter rispedire al mittente il prodotto. Per le automobili, qualcosa di simile: il codice deontologico dice che non si dovrebbero vendere automobili, e per il colore e per il prezzo. Sulle transizioni via internet, infatti, al massimo è possibile spendere 20000 euro (a causa delle leggi anti-riciclaggio). Si noti che questo è un limite cumulativo: non è possibile comprare più oggetti dallo stesso venditore con la stessa transazione e superare i 20000 euro. Si ha inoltre a che fare con il UIC, ossia l'Ufficio Italiano Cambi, che controlla ciascuna transizione, in accordo tra la Banca di Italia e con il Ministero delle Finanze; nel momento in cui si hanno transizioni su website con la triangolazione utente-website-banca, il dato non è neutro: quando il limite della transizione si avvicina ai fatidici 20000 euro, o si ha a che fare con beni delicati, il UIC fa segnalazioni alla Banca di Italia e alle Finanze, che fanno controlli sul codice fiscale controllando i conti a disposizione, studiando eventuali illeciti. Quello che si può fare tuttavia aggira questo problema, ovviamente legalmente, introducendo una seconda fase: sul web è possibile prenotare un incontro per la visione dell'oggetto, dell'automobile, in cui si può vedere e provare, quindi pagare in contanti. In caso di errore si può (in questo e negli altri casi) scrivere al venditore e cambiare, o riavere indietro i soldi, entro 10 giorni[1], ma solo per quanto riguarda la vendita di prodotti.

[1]Si noti che i supermercati e i negozi possono scegliere, a propria discrezione, di ampliare il termine, restituendo i soldi anche entro 15/30 giorni

Nel caso di servizi, quale ad esempio una consulenza, ciò non è possibile: se si richiede una traduzione, un software, non esiste un termine di recusazione, dal momento che per legge la domanda non è opponibile: i servizi sono attività certe, definite, su cui l'utente non può aver dubbi al momento della richiesta: occorrerebbe dimostrare malversazioni, costrizioni, o simili, cosa legalmente mai riuscita. Una volta dimostrata la chiarezza sul protocollo, la localizzazione della società, si potrebbe teoricamente fare, altrimenti no.

Quando i boss della malavita comprano con milioni di euro, ciò che si fa è pagare mediante conti bancari esteri, su paradisi fiscali. Tendenzialmente comunque, all'interno dell'UE, è impossibile "fare i furbi" in questo modo, dal momento che, per grosse somme, i controlli sono molto stretti e rigidi.

Nota finale: se l'utente si accorge che cade la linea e/o qualcosa non va, finchè non si effettua un'autorizzazione finale, al termine di un certo numero di richieste, è possibile annullare la transazione. Ovviamente, i dettagli della cosa dipendono dal protocollo utilizzato, e da quando il provider/negozio permette la possibilità della conferma definitiva dell'acquisto.

Capitolo 4

Lezione 04 : 08/06/09

In questa lezione gli argomenti principali sarà fondamentalmente la firma digitale/elettronica/elettronica avanzata, riprendendo alcune nozioni dalle lezioni precedenti.

4.1 Firma digitale/elettronica

La prima normativa riguardante la firma digitale fu la 99/93/CE, dunque una direttiva europea, alla quale si dovevano conformare le varie legislazioni nazionali. La normativa fondamentalmente riguardava la vidimazione degli atti in linea informatica in modo da rendere i documenti informatici del tutto equipollenti a quelli cartacei. Si introduce inoltre il concetto di:

- Firma digitale;
- Firma elettronica;
- Firma elettronica avanzata.

Per "firma elettronica avanzata", si intende una firma elettronica "forte", dalla validità inconfutabile; per "firma digitale" si intende al contrario la più debole; esistono differenze tra firma elettronica ed elettronica avanzata, che verranno presentate tra breve. In Italia la definizione e la validità delle tre firme è definita nel decreto legislativo 10/2002: la regolamentazione giuridico/tecnica della firma digitale.

Si arriva ora al nocciolo della questione: lo scopo della firma digitale è documentare che chi ha scritto qualcosa si assume la responsabilità del contenuto di ciò che ha scritto; ciò che si vuole intendere per "attribuire la responsabilità " è dire che qualcosa sia non confutabile e non opponibile.

Tradizionalmente, per ottenere un documento di questo genere, è necessario rivolgersi a un notaio il quale, per mezzo di documenti e/o in presenza di due testimoni, dichiara che la persona che firma gli atti è effettivamente quella persona, rendendo la firma di fatto non confutabile e non opponibile, dunque valida per qualsiasi atto, per sempre.

Cosa si fece dunque, per garantire qualcosa di simile per documenti informatici, riducendo ovviamente le difficoltà ? La prima idea fu quella di utilizzare alcuni applicativi in grado di produrre una firma digitale; un'idea iniziale (ovviamente molto poco utilizzata) fu quella di scannerizzare una firma e apporla sui documenti informatici; si produssero poi firme più affidabili, ma comunque assolutamente opponibili.

Storicamente, si torna al 1967, in cui si iniziò a pensare a una modalità differente di gestione della firma, al fine di evitare notai e anagrafe; Cassese e Bassarini modificarono le caratteristiche della firma cartacea non tanto per motivi di sicurezza, quanto per motivi tecnologici: nell'ambito degli ordini (automobili, pezzi di ricambio), per questioni di pagamenti, si iniziò a utilizzare i fax. Un ordine veniva fatto su carta, veniva vidimato dai vari responsabili, il venditore lo acquisiva e si attendeva una conferma dopo richiesta. Riassumendo, si avevano tre passi:

1. Ordine;
2. Ricezione ordine e richiesta di conferma;
3. Conferma.

Dall'avvento dei fax iniziò a circolare meno carta, cosa sicuramente positiva, ma non particolarmente sotto il punto di vista della sicurezza: un fax poteva essere tranquillamente alterabile, per quanto l'inserimento di un terzo nella transazione fosse altamente improbabile.

Fu compito dell'AIPA (oggi CNIPA) quello di introdurre una maggior regolamentazione in questo ambito, cercando di ridurre i problemi sotto questo punto di vista: il fax fu superato dalle stazioni informatiche, e di qui si cercò di rendere validi acquisti anche corposi, in modo da incentivare anche il commercio elettronico. Una modalità utilizzata solo temporaneamente fu quella di effettuare una dichiarazione da parte dell'acquirente, mediante una lettera che veniva firmata, scannerizzata, trasmessa come immagine. Come già detto, una forma di comunicazione di questo tipo è banalmente alterabile: è possibile ricavare la firma da un documento, riutilizzarla, modificarla a proprio piacere.

La grande innovazione sotto il punto di vista della sicurezza fu la direttiva del 1999, e in Italia il decreto legge del 2002, che stabilirono i puntelli della

firma digitale: per i primi due anni circa di fatto si continuò con la strada del "foglio scannerizzato", in attesa di ideare tecniche migliori.

Era necessario trovare delle modalità , offerte da tecnologie ideate da alcuni personaggi fondamentali per la storia della teoria dei codici (Diffie-Hellman, Rivest-Shamir-Adleman, e altri): mediante algoritmi particolari si poteva generare qualcosa di equivalente a una firma, ottenendo però qualcosa di molto interessante: qualcosa di estremamente difficile da duplicare, da imitare, da modificare e riprodurre a proprio piacimento, introducendo dunque la possibilità di rendere la firma sicura sotto il punto di vista della sua veridicità , dunque anche sotto il punto di vista della sua non opponibilità.

L'idea, a partire da questi algoritmi, è quella di generare firme sempre diverse a seconda delle persone, e dell'istante di tempo in cui vengono generate. Tutto si basa sul concetto di "hash", ossia di una sorta di "impronta" che sarà sempre diversa anche dal punto di vista dell'istante di tempo in cui viene generata. Mediante una "marca temporale", si riesce a generare in una data certa, sicura la firma, in modo da renderla di fatto non opponibile, proprio come la firma depositata da un notaio.

Ci si potrebbe chiedere a questo punto:

- Chi emette la marca temporale?
- Si ha la possibilità di forzare l'algoritmo, in modo da riprodurre una firma digitale?

L'autorità che rilascia i certificati per la firma elettronica (non per la marca temporale) è la CA, ossia "certification authority". Essa permette a una persona fisica o giuridica di poter utilizzare, contrassegnare un documento mediante una firma elettronica. Conoscendo le regole del rilascio di codice fiscale e partita IVA, il codice fiscale rappresenta una persona fisica, la partita IVA una persona giuridica. Nel momento in cui le aziende devono colloquiare con altre aziende, la partita IVA viene fornita come dato a un'azienda, ma dietro non ci sarebbe nulla se non vi si associasse una persona fisica, ossia un codice fiscale.

L'Italia ha obbligato a informatizzare il trasferimento dei bilanci; dal momento che non è sempre possibile avere un notaio a portata di mano, si dovette introdurre la firma elettronica, creando due autorità, una delle quali è la già citata CA, l'altra è la SA (che si discuterà dopo). In America c'è il NIST; in Europa c'è il CENELEC e l'IST, affiliate alla ANSI e alla IEEE.

Ci sono alcuni problemi: le CA possono rilasciare l'autorizzazione alla firma elettronica a qualunque utente che faccia parte alle nazioni. Non ci fosse nella nazione un'ente in grado di fornire l'autorizzazione, si potrebbe chiedere

l'autorizzazione a un'altra nazione: dal momento che gli elenchi sono pubblici e internazionali, non si dovrebbe avere problema. La non opponibilità, non disconoscibilità della firma, garantite tra più CA, sono realizzate grazie alla interoperabilità: chi riconosce una firma elettronica e la introduce in un catalogo, può far vedere a qualsiasi altro ente lo stesso nominativo, in tutti i paesi, presentando gli algoritmi utilizzati per la generazione della firma e altre informazioni.

Potrebbe capitare che l'azienda sia in stato di falso in bilancio, o abbia effettuato un dolo del qualche tipo, dunque la CA deve bloccare la validità della firma, avvertire il ministero delle finanze e le enti interessate. Se la CA blocca la firma, da lì in poi tutte le operazioni fatte vengono bloccate e/o controllate. Nel caso al contrario sia la CA a effettuare sgarri, si toglie la suddetta dall'elenco dell'interoperabilità. In questo modo, tutti i suoi certificati vengono bloccati. Nel caso la colpa tuttavia fosse solo delle CA, si ingloberanno nelle liste di altre CA, o di enti sovranazionali, le firme che devono essere validate, permettendo ai detentori delle suddette di poter andare con un altro certificatore; si emetteranno in questo periodo di transizione certificati temporanei, in modo da "coprire i buchi".

In ogni CA esistono tre registri:

- Firme presenti: firme elettroniche valide e utilizzabili a tutti gli effetti;
- Firme sospese: la sospensione è a tempo, determinato: 3, 6 mesi;
- Firme revocate: firma invalida a tempo indeterminato.

In Italia ci sono 19 certification authorities, ossia associazioni in grado di generare e gestire firme elettroniche.

Una CA deve acclarare il fatto che al momento della trasmissione di un bilancio, per esempio, sia stato tutto effettuato in modo corretto rispetto a ciò che la legge impone; in tale direzione dovrà intervenire anche la seconda società fondamentale per le firme elettroniche: la SA (Stamping Authority), ossia la società che, su richiesta della sua utenza o di una CA, rilascia un "bollino" in cui si afferma che la trasmissione è stata effettuata a una certa data/ora, generando un'impronta che andrà inserita nel documento, crittata.

Le CA sono come dei notai virtuali, ossia enti privati riconosciuti dagli stati. Si tratta di autorità terze parti che intervengono nella trasmissione di dati sicuri.

La firma digitale (nel vero senso della parola) è assolutamente obsoleta, ma in alcuni documenti essa è citata al posto della firma elettronica o della firma elettronica avanzata. Si mandò un invito al legislatore a chiarire, dal

momento che cattive interpretazioni possono comportare problemi al livello dell'interpretazione della legge.

Quali sono le differenze tra firma elettronica e firma elettronica avanzata? Beh, fondamentalmente, l'unica differenza sta nella difficoltà nello scardinare l'algoritmo, ossia nella sicurezza della chiave: mediante una chiave privata si genera una firma elettronica, ossia una sequenza di bit; nel caso di una firma elettronica avanzata si ha dunque una maggior forza dell'algoritmo, ossia è necessario un tempo molto più elevato per scardinarlo. I passi sono i seguenti:

1. Si sceglie quale algoritmo utilizzare per la generazione della chiave;
2. Scelto l'algoritmo si genera la chiave;
3. A partire dalle precedenti, si genera una firma elettronica mediante un hash, ossia mediante una sorta di "impronta".

Le chiavi sono state usate nel tempo partendo da algoritmi sempre più forti; un tempo si utilizzavano coppie di chiavi simmetriche, ora asimmetriche: dal momento servono chiavi sia per la generazione dell'impronta sia per l'interpretazione, un tempo esse erano sostanzialmente uguali, simmetriche, ora per maggior sicurezza si tende a utilizzarle diverse. Se un algoritmo generasse un "programmino" in grado di generare firme, questo si potrebbe fare se la chiave privata (Key_S) e la chiave pubblica (Key_P) fossero uguali.

L'algoritmo di Diffie-Hellman permette di avere una buona robustezza anche con chiavi simmetriche; ciò significa che è come se nella mia borsa avessi le chiavi dell'albergo, ma gli inservienti il passe par tout. Nel caso di un sistema molto sicuro la chiave private deve essere esclusivamente a disposizione dell'utente, neanche a disposizione della CA (che al contrario avrà nei propri elenchi la chiave pubblica); la CA deve conoscere chiave pubblica e algoritmo, assolutamente non la chiave privata.

La sicurezza in realtà sta in un altro fatto: bisogna essere in grado di denudare le varie impronte che transiteranno sulla rete al momento dell'uso della chiave: chiave + hash della CA più hash della SA + hash del documento. Ciascun documento è composto sostanzialmente in quattro elementi, ciascuno univocamente associato agli altri. Il documento viene dunque "spezzettato", dunque, senza conoscere i dati, è impossibile interpretarlo, dal momento che mancano le informazioni per poterlo "ricostruire". Quando si trasmette qualcosa, si invia solo parte del documento, in maniera crittata, e a questa parte si associano le hash di SA e CA. Si generano impronte che rendono decodificabili la firma, la data, l'ora, il server di partenza. Gli algoritmi più moderni sono ES-HA1 e DES, ossia un'evoluzione di quelli precedenti.

Una volta effettuata la trasmissione, dei segnali di controllo tolgono dalla rete il documento, dal momento che ci può essere stata un'intrusione da fuori o da dentro (nella fattispecie, il 70 % delle intrusioni sono proprio interne alla rete dove si lavora).

Come si trasmette la chiave? La trasmissione viene effettuata mediante un algoritmo non noto se non alla CA; a partire da queste istruzioni si genererà una chiave, da parte dell'utente, chiave che nessun altro potrà conoscere. Per generare la chiave la CA trasmette un software in grado di generare la suddetta chiave; nel caso le chiavi siano simmetriche, esse sono teoricamente uguali, ma generate in modo diverso, dunque recuperarle non è comunque facile. Ciò che di solito un hacker cerca di fare è lavorare sul documento, sull'informazione, non sulla firma. Nel caso delle chiavi asimmetriche, tuttavia, neanche la CA è in grado di ricostruire la chiave privata, poichè queste vengono elaborate solo sulle macchine dei singoli utenti, aumentando la sicurezza.

Lungo la rete viaggiano informazioni "monche", spezzate: le informazioni non sono complete e tantomeno in chiaro, bensì spezzettate, in modi particolari; si fa in modo che solo il destinatario sia in grado di ricostruirle, mediante un processo di chaining, conoscendo l'ordine corretto per la ricostruzione.

4.2 Cenni sulla PEC

Si vuole a questo punto introdurre i passi necessari per ottenere un sistema di posta elettronica certificata, senza approfondire eccessivamente l'argomento.

1. Al momento della trasmissione, il server del mittente prende il carico la mail;

2. Presa in carico la mail, si inoltra una ricevuta al mittente, certificando il fatto che la mail è presa in carico;

3. Si effettua un controllo antivirus e di altri tipi; se negativo il messaggio viene conservato in quarantena per trenta mesi, quindi si dice che il messaggio non può essere inviato, segnalandolo al mittente;

4. Nel caso il controllo abbia esito positivo, si controlla che ci sia spazio, dal server del mittente a quello del destinatario; se la risposta è positiva, si manda richiesta al server del destinatario di poter trasmettere il messaggio, chiedendo se la ricezione è possibile;

5. Nel caso il destinatario accetti, il messaggio viene preso in carico dal server del destinatario, e si manda una ricevuta di corretta ricezione sulla presa in carico;

6. Sul server di partenza, una volta aperto il file, si riceve una notifica del fatto che il messaggio è stato preso in carico dal destinatario, e aperto.

Di tutta la mail, il messaggio (header) è l'unica parte che viaggia in chiaro; gli allegati sono rigorosamente crittati. Gli allegati del documento sono tutto ciò che non è header; essi sono:

- Certificato di autorizzazione della CA a mandare messaggi sicuri (l'hash è parte dell'allegato);
- Certificato di trasmissione a una certa ora (hash di timestamp) da parte della stamping authority;
- Hash di documento parziale;

Per la PEC avverrà qualcosa di analogo alla firma elettronica: si avranno chiavi private e pubbliche, in grado di crittare e decrittare il messaggio, verificandone l'autenticità.

Capitolo 5

Lezione 05 : 15/06/09

La presente lezione tratterà due argomenti: la carta di identità elettronica, e il diritto alla proprietà intellettuale.

5.1 Carta di identità elettronica

Parlando di documenti e documentazione, è necessario che essi abbiano una validità; per definire la validità è necessario, di conseguenza, introdurre una certa legislazione.

Si consideri una banconota da 10 euro tagliata e riattaccata: essa, di fatto, non vale più 10 euro, non vale più nulla: per legge, solo se integro il documento vale qualcosa. Se una banconota viene riattaccata e i due seriali sono uguali il valore legale esiste, nel senso che in banca si può ottenere a partire da essa una banconota nuova di eguale valore (idem per le monete), ma non si può utilizzare per scopi commerciali.

Un discorso di questo genere, sulla validità e sui contesti di validità dei documenti pubblici, è stato applicato all'estero e in Italia da diverse nazioni. In base a una legge del 1968, in Italia si iniziarono le prime applicazioni nel 1997, dunque vennero introdotte nuove leggi nel 2002. La normativa in questione riguarda la semplificazione della procedura per il riconoscimento dei cittadini (in tal caso, italiani): si intende introdurre dei badge che permettessero la sostituzione della carta d'identità tradizionale, in modo che essa possa contenere le informazioni necessarie, ossia una serie di puntatori in grado di accedere a diversi database elettronici.

Si fecero esperimenti su di un materiale che potesse non essere cancellabile, potesse essere resistente all'abrasione da sforzo, resistente ad acidi. Lo stratagemma utilizzato per le carte di identità elettroniche è stato quello di utilizzare strutture multistrato, nella fattispecie a 5 strati: uno di velina,

uno di sostegno, uno che contenga alcuni caratteri, un altro che contenga i caratteri più importanti, un ultimo di sostegno al resto della matrice: una struttura multilayer. Il primo materiale utilizzato era l'ABS, che però non era un granchè, dal momento che molto spesso si rompeva.

Con la sola carta di identità elettronica si potrebbe fare in modo da sostituire carta di identità, codice fiscale, tessera sanitaria, patente; l'idea fondamentalmente era "copiare" l'idea dei bancomat: avendo sulla carta nome, cognome, data e luogo di nascita, codice fiscale, firma, data di validità, ologramma come strumento di non falsificazione, si può ottenere un'alternativa valida a tutti i documenti. La carta può avere un costo sui 30 euro e può essere rilasciata dall'anagrafe o da uffici esterni autorizzati. Nello stesso database cui si introducono i dati della carta di identità si potrebbero introdurre molte altre informazioni, quali la firma digitale/elettronica. La partita IVA assolutamente no: a una partita IVA deve essere associato un certo codice fiscale, non il viceversa.

I vincoli per questa carta di identità elettronica sono molteplici:

- Tempi per il rilascio e per la messa in moto di tutti i servizi;
- Costi per il rilascio;
- Possibilità di accordare tutti i vari servizi.

Si decise di fare un primo esperimento a Parma, città nella quale si accordarono anagrafe, ministero, banche, trasporti, ASL, IVA, così che tutte le persone che lo desideravano potevano sostituire gratuitamente la carta di identità con quella elettronica, ottenendo la possibilità di usarla in tutte le possibili applicazioni. L'esperimento riuscì, ma ci furono dei difetti: il costo del materiale è molto elevato, circa 30 euro a persona, inoltre la tecnologia per trattare il medesimo materiale è molto costosa, le normative da rispettare rigide, dunque anche il numero di fornitori/trattatori di materiale è molto limitato: il ministero non avrebbe assolutamente potuto coprire richieste a livello nazionale.

Si approvò una variante: la carta elettronica con chip, anzichè banda magnetica: il chip permette di avere una memoria maggiore, una minore facilità di alterazione, permettendo un'aggiornabilità istantanea. Nel caso si cambi la residenza, è sufficiente aggiornare la carta con il chip e ottenere una carta di identità rinnovata. Il chip è molto capace, per quanto non illimitato, ma non è autoaggiornabile: è necessario, per ciascuna amministrazione, fare in modo che essa possa trattare e aggiornare solo i dati che la competono; la ASL aggiornerà solo dati sanitari, l'anagrafe anagrafici, e così via.

Aggiungere molti servizi alla stessa carta non è semplice: per quanto elevata, la capienza del chip è comunque limitata, dunque i servizi aggiungibili sulla medesima carta dipendono dalla capienza del chip: a ogni aggiornamento di fatto si aggiungono dati, dal momento che si tende a mantenere intatta la storia dell'individuo, a tenerne traccia. Tendenzialmente, per una banca per ogni conto corrente si possono avere più carte, ma non più una carta per due conti correnti; oltre che per motivi di sicurezza, questo fatto è dettato per motivi di capacità del chip.

Nel momento in cui capita che il documento è "full", ossia non più aggiornabile, l'operatore deve informare che non si ha più la possibilità di aggiornare, dunque richiedere all'ente che ha rilasciato il documento il cambio di carta.

5.2 Diritto alla proprietà intellettuale

La nascita di un diritto finalizzato alla regolamentazione della proprietà intellettuale nasce quando nasce la consapevolezza della necessità di proteggere ciò che si produce (scritti, musica, video).

Un primo problema potrebbe riguardare il diritto riguardo opere molto antiche (quali opere di Mozart, Beethoven, Schubert): nel caso tutti i discendenti dei musicisti fossero deceduti, l'opera non diventa "priva" di diritti, ossia liberamente acquisibile, poichè in queste situazioni, quantomeno molto frequentemente, i diritti vengono attribuiti a fondazioni nazionali: in Germania o Austria dopo la morte degli ultimi eredi dei suddetti musicisti, ad esempio, lo stato tedesco decise di fondare le fondazioni, che esigessero il diritto a proprio uso per l'esecuzione e la registrazione delle opere. I profitti dai diritti vengono utilizzati per elargire borse di studio, a scopo prevalentemente musicale.

Discorsi del tutto analoghi sono applicabili anche in campo scientifico: nel caso di brevetti scientifici, esistono fondazioni per esempio legate alla figura di Guglielmo Marconi: diverse fondazioni sfruttano i diritti derivanti dai brevetti di Marconi per produrre fondi di ricerca o borse di studio. Università tecniche quali il MIT, Berkeley, il Politecnico di Torino / Milano, producono molti brevetti all'anno, il ricavato dal cui utilizzo viene impiegato in diversi modi.

Se una persona è al di fuori di un'istituzione, i diritti sono esclusivamente suoi; nel caso tuttavia la persona produca un brevetto legato ad un'attività legata all'istruzione, è necessario vedere com'è collocata la persona che produce l'opera di ingegno; istituzione e persona hanno un contratto che fa riconoscere reciprocamente delle condizioni di sfruttamento del brevetto.

In Italia si ha un'ente, nota come SIAE, che gestisce i diritti, fornendo la legislazione e riscuotendo i diritti; ha senso o meno, rispetto alla tecnologia e alle tradizioni attuali, un'ente di questo genere? Beh, alcuni anni fa si tentò di eliminare la SIAE in quanto spesso inutile, anche se essa risultò essere utile in alcune vicende di 15 anni fa. In varie città italiane, soprattutto a Napoli e Torino, si trovavano molti prodotti masterizzati senza bollino SIAE, o con una versione falsificata del medesimo. In seguito all'enormità di produzione di supporti di questo genere, il ministero si mosse in una direzione discutibile: vennero raddoppiate le tasse sul bollino sui vari prodotti, comprendendo tuttavia anche i supporti vuoti, vergini. Se un supporto è vuoto, non ha senso tassarlo, dal momento che non vi è nulla da proteggere: la SIAE ha diritto ad entrare in azione dal momento che il supporto contiene informazione, e neanche di tutti i tipi: tutto ciò che viene esclusivamente prodotto e registrato in via privata, non tocca in alcun modo la SIAE.

Esistono due "filosofie", due "parrocchie", per quanto riguarda la legittimità nel chiedere di pagare un diritto, e come pagarlo, in base a quali parametri: DRM e CC. La legge internazionale afferma che chi fa visualizzare un link, da qualche parte deve precisare che l'utente che accede deve leggere un contratto che appare automaticamente. Una cosa spiacevole che può capitare è il fatto che qualcuno riesca a effettuare il downloading senza che prima si accetti il contratto, effettuando un reato. La portata del dolo dipende dal fatto che ciò che è stato fatto sia stato fatto in modo malevolo e/o con artifici tecnici, e sulla base dell'importo del costo del bene e del profitto che si può realizzare si può portare il reato dall'essere civile all'essere penale, con diverse sanzioni aggiuntive.

Ciò che si può generalmente fare, ad alcune condizioni, è scaricare materiale da internet per uso personale, e utilizzare da solo le medesime; una volta che si condivide, il reato è per tutti quelli che condividono. Per quanto riguarda il salvataggio su supporto ottico/magnetico di materiale illegale procurato da internet, sulla legislazione esiste una grossa confusione: innanzitutto sul sito dal quale viene effettuato il download devono essere specificate, al fine di rimanere in legalità, le condizioni e i vincoli imposti sul materiale presente in rete.

Alcune case editrici hanno liberalizzato alcuni romanzi (è molto improbabile che le case discografiche facciano altrettanto); idem alcune case produttrici di software, idem un grosso motore di ricerca, ma poi sono stati creati casi molto difformi tra loro, generando una grossa confusione. Un caso estremamente particolare è quello di questo motore di ricerca: esso ha messo a disposizione intere compilation, ma ciò ha permesso è stato far scaricare alla gente una quantità enorme di materiale: dopo due o tre giorni i proprietari del motore di ricerca hanno interrotto tutto, ma due o tre giorni per la rete

è un tempo lunghissimo.

Come già detto, esistono due filoni, due filosofie: DRM e CC.

- DRM (Digital Rights Management): si tratta di una scuola di pensiero secondo cui tutto il materiale va tendenzialmente bloccato (diciamo come politica di base), liberalizzando esclusivamente alcuni materiali, che devono essere esplicitamente indicati come "liberi". Ciò tende a bloccare qualsiasi possibilità di download, a meno che ovviamente non si effettui un pagamento.

- CC (Creative Commons): per Creative Commons si intendono delle "regole comuni sulla creazione di un qualcosa": l'autore deve stabilire fino a quale punto intende veder riconosciuti i propri diritti, dunque introducendo un riconoscimento parziale; esso non può comunque disconoscere completamente il diritto. L'idea è comunque quella di selezionare solo parte dei diritti, e liberalizzare le restanti possibilità.

Capitolo 6

Lezione 06 : 22/06/09

Verranno mostrati a questo punto alcuni concetti espressi nella lezione.

6.1 Reti telematiche

Chi mette a disposizione una certa rete telematica al fine di fornire un determinato servizio deve essere un terzo, ossia una società terza sia allo stato sia ai gestori di rete. Questa è una norma che in Italia non viene rispettata: la rete dovrebbe essere associata per forza ad una determinata società per azioni. In Italia le frequenze UMTS sono state vendute a prezzo elevatissimo, dallo Stato, al fine di guadagnare su di esse. A questo punto sarebbe necessario, per tutti gli utenti, effettuare direttamente un'identificazione. Per quanto riguarda le reti, tuttavia, è stato introdotto un tal numero di utenti, da ottenere alcuni effetti. Ciò che si deve fare, in sostanza, è rispettare i seguenti due punti:

- Mappare e definire le caratteristiche delle reti telematiche, dunque la loro architettura;
- Identificare le macchine degli utenti che utilizzano la rete; dal momento che, come accennato, vi è un'enormità di utenza, l'identificazione degli utenti è stata assegnata ad enti esterni, che potessero effettuare questo tipo di operazione.

Capitolo 7

Lezione 07 : 29/06/09

In questa lezione verranno soprattutto riprese precedenti lezioni, introducendo tuttavia alcune novità, riguardo i sistemi di sicurezza.

7.1 OECD Guidelines

Uno dei documenti pubblicati riguarda l'OECD: si tratta di guidelines, non di normative. L'OECD è un'organizzazione riguardante lo sviluppo economico; il documento indirizza i paesi dell'Europa e quelli associati o affiliati (quali Svizzera o Israele): paesi come questi pagano dei diritti per avere benefici dalla comunità allargata (ossia Comunità Europea + affiliati).

Il commercio elettronico viene visto e favorito, come già detto, in modo diverso a seconda del paese in cui ci si trova; Italia e Belgio erano inizialmente paesi estremamente rigidi sotto il punto di vista della normativa, la Francia con leggi un po' meno stringenti (dal motivo che grossi gruppi commerciali spingevano per aprire le frontiere al commercio elettronico, per quanto ora di queste aziende sia rimasto poco in tale ambito); dopo la caduta delle grosse aziende, si decise di irrigidire le regole.

Ciò che emerse, in totale, è il fatto che sia l'acquirente sia il venditore non se ne fanno niente di regole da poco, dunque stringerle è abbastanza fondamentale, al fine di ottenere un certo insieme di garanzie reciproche. SSL3 ha permesso di avere triangolazioni molto più sicure ed efficienti rispetto a prima; ora si ha molta rigidità ovunque per quanto riguarda il commercio elettronico, e oltre alle linee guida sono introdotte normative altrettanto rigide.

7.2 Carta di identità elettronica

Per quanto riguarda la carta di identità elettronica, si vogliono solo fare alcune precisazioni ulteriori: come validità si ha qualcosa di pari a quella cartacea (dunque intorno ai cinque anni); a meno di particolari casi, quali il valere delle leggi al momento dell'emanazione del documento, la prassi è questa.

Per i minorenni esiste un equivalente, ossia la carta DIE (Documento di Identità Elettronico), ossia una sorta di carta bianca elettronica. La carta bianca e la carta regolare possono (ma non devono) essere valide per l'espatrio, se ovviamente è stata effettuata la richiesta di autorizzazione al momento della richiesta del documento; se la carta non è valida per l'espatrio, non è possibile andare nemmeno in paesi dell'Unione Europea. La dicitura "valida per l'espatrio" permette di identificare le carte valide da quelle non valide in tal senso; se la carta è valida per l'espatrio, è possibile muoversi liberamente in ciascuno dei 27 paesi dell'UE (nonchè nei paesi affiliati quali Malta e altri). Si noti che per la validità per espatrio non è sufficiente un'autorizzazione dal solo comune: al fine di poter avere tale validità, è necessaria un'autorizzazione anche da parte della Questura.

La DIE può essere associata solo ai genitori: se non è presente un tutore del ragazzo, essa non ha validità. Per i ragazzi dai 15 ai 18 anni non è possibile emettere carte di identità elettroniche: vi è, in tal senso, un vuoto legislativo (è possibile solo avere carte di identità cartacee).

7.3 Sistemi di Sicurezza

Nell'ambito della sicurezza informatica, con le reti che trasmettono dati riservati, esistono norme tecniche (non allegate nell'allegato tecnico CNIPA) che riguardano ambienti di questo tipo.

La prima cosa che viene fatta, ad esempio per comunicare tra un ministero ed un altro, un ministero e una banca e simili, è effettuare una distinzione tra due tipi di reti: rete "aperta", ossia in cui è possibile un accesso esterno, e "chiusa", in cui l'accesso esterno è impossibile. Reti aperte e reti chiuse non possono essere assolutamente comunicanti tra loro, per legge, al fine di evitare intrusioni.

La rete chiusa funziona sostanzialmente su di una LAN privata, facendo in modo che i flussi non escano da essa. Si tratta di una LAN che potrà collegare per esempio una filiale con le agenzie, e così via. Esistono organi esterni che possono controllare reti di questo tipo, vigilare su di esse e regolamentarle, quale ad esempio il CNIPA. Un client non deve essere in grado di alterare

le informazioni presenti su di una rete; i server invece ragionano "a fette", dividendosi il lavoro.

I server sono macchine molto complesse, in numero generalmente plurimo (operanti in modalità RAID, Redundant Arrays of Disks); i dischi contengono informazioni anche ridondanti, in modo che si possa fare manutenzione a caldo, "hot replacement", senza dover quindi spegnere la macchina e sospendere il servizio. Esistono macchine in open space a disposizione di più persone (come anche stampanti: presto si parlerà di stampanti di reparto che potranno funzionare dopo l'identificazione mediante smart card e/o user/password).

Il server si trova in una MZ, ossia in una zona militarizzata, dal momento che si mettono in pista tutte le tecniche per la protezione dai danni della macchina. Prima di tutto la sicurezza deve essere sotto il punto di vista della corrente elettrica: utilizzando degli UPS è possibile proteggere la macchina da sbalzi e da black out; i sistemi di protezione sono firewall, antivirus (i quali devono essere utilizzati almeno una volta al giorno per scansioni, per esempio al mattino o alla sera, quando nessuno lavora).

Qualcuno deve poter uscire da ciascuna sotto rete, altrimenti non è possibile acquisire dati da alcuna parte. Tra la rete MZ e la rete DMZ (zona demilitarizzata) devono esistere connessioni, mediante proxy che le collegano. Per zone MZ e DMZ si parla sempre e comunque di reti chiuse, dunque per quanto si parli di zone più o meno militarizzate, si considera sempre di dialogare con macchine esterne, ma comunque autorizzate e facenti parte della rete chiusa.

Una rete DMZ è apparentemente non protetta, ed è costituita da macchine non molto sofisticate: esse sono di fatto dei collettori di dati in ingresso e uscita: ciò che serve per queste macchine è una grossa disponibilità di memoria al fine di accumulare un grosso numero di dati, tuttavia la presenza di una grossa potenza di calcolo è assolutamente inutile, dal momento che le elaborazioni non avvengono in essa. Si parla in sostanza di grossi parcheggi di dati, come delle grosse buche delle lettere. Le macchine adibite a collettori di dati vengono dette "bastion host": si tratta di macchine che possono raccogliere dati, non possono trasmetterne, e non possono effettuare elaborazioni.

Il proxy invierà alla macchina esterna l'ordine di prelevare dal "box" questi documenti; i documenti sono prelevati dunque in maniera pressochè istantanea: essi restano nel box per un certo tempo in modo da filtrare il contenuto, dunque solo dopo i dati utili vengono prelevati per pacchetti omogenei. Si noti che solo nella rete chiusa, una volta filtrati tutti i problemi, è possibile far transitare più pacchetti alla volta.

Il punto della rete più interessante da attaccare (e attaccabile) è il proxy: si sa che i proxy sono i piloti delle informazioni; essendo in grado di lavorare sul proxy, dunque, si potrebbe entrare nei server interni. I proxy sono di fatto le macchine più potenti, dal momento che devono gestire il transito dei dati per la rete. Mediante un sistema di logging è possibile osservare i tentativi di hacking, sniffing, spoofing e attacchi di altro tipo.

L'obiettivo di un hacker potrebbe essere quello di intrufolarsi dove non si è autorizzati al fine di rubare dati, identificazioni o altro, come indirizzi IP. Gli altri termini possono riferirsi ad altri tipi di danni, ad esempio cattive identificazioni, spionaggio di pacchetti o altro.

All'inizio si scelse di non utilizzare eccessivamente la crittografia; ora per moltissime applicazioni essa è obbligatoria per legge (nei contesti di banche, comunicazioni tra aziende, ministeri e quant'altro). Solo parte dei messaggi è trasmessa in chiaro, il resto è crittografato mediante procedure note o anche non note: sembra di fatto di trasferire in chiaro ma i programmi utilizzati di fatto crittano, non permettendo nemmeno agli utenti o agli impiegati di avere informazioni riguardo questo procedimento. I sistemi utilizzati ad esempio sono il DES (algoritmo ancora molto forte; utilizzare algoritmi più avanzati potrebbe richiedere costi eccessivi, dunque si sceglie di rimanere ad esso, molto spesso).

Fenomeno che avviene sempre più frequentemente è lo spamming: trasmissione di molte email su mail private o di servizio, intasando il servizio; esistono tecniche in grado di far creare spam sulle caselle di rete, per quanto queste siano tendenzialmente bloccabili.

7.4 Note conclusive del corso e risposte/chiarimenti

Verranno ora elencate alcune risposte ad alcune domande fatte, in modo da chiarire alcuni eventi.

- Nella legge 675/1996 si aveva ordine tra dati generali, semisensibili e sensibili. Con la 196/2003 si è perso parte di questo ordine. Per dati semisensibili si intendono dati in cui la legge permette o meno di renderli pubblici a seconda delle situazioni.

- Marche temporali: le marche temporali vengono fornite dalle stamping authority; spesso esse sono enti terzi, a volte anche sottodipartimenti delle CA stesse.

- Ciò che è stato detto per il commercio elettronico richiede un chiarimento: chi vuole operare in qualsiasi nazione deve essere autorizzato

in quella nazione, e non solo nella propria; una procedura di questo tipo deve esistere anche quando vi sia reciprocità di diritto. Ebay o Amazon hanno uffici nelle varie nazioni, dove la gente può andare per reclamare: esistono autorizzazioni scritte perchè ci sia rappresentazione nelle varie nazioni, ossia una rappresentanza fisica e/o legale/giuridica. Per quanto riguarda il commercio elettronico, si ricordi che si può fare un acquisto di prodotti/servizi sulla rete, e una volta completato l'acquisto si ha un codice che ha anche valore legale. Il tempo di recessione è fisicamente di 7 giorni, per acquisti elettronici 10. Se si ha già pagato, dal corriere si deve prendere dal momento che esso è un terzo, ma si dovrà rispedire a proprio carico. Si ricordi che il servizio non può essere ripagato.