Questo articolo è apparso sul Corriere del Ticino di lunedì, 19 febbraio 2001 nella sezione Informatica e Sicurezza

Internet: ci aiuta la crittografia

Il sistema a doppia chiave garantisce la protezione nello scambio dei dati

Silvano Marioni **www.marioni.org**

Il successo delle transazioni commerciali su Internet dipende dai medesimi meccanismi di sicurezza che utilizziamo quotidianamente nel mondo reale.
Anche su Internet desideriamo assicurarci dell'identità dell'interlocutore con cui comunichiamo e vogliamo avere la garanzia che i dati inviati sulla Rete mantengano la loro riservatezza e la loro integrità. Infine abbiamo bisogno di accorgimenti che garantiscano i contraenti da possibili contestazioni e impediscano la ricusazione delle transazioni effettuate.
Su Internet possiamo avere queste garanzie utilizzando delle tecniche particolari di crittografia.
Da sempre la crittografia permette la comunicazione protetta tra due interlocutori, trasformando un testo in chiaro in un testo cifrato, incomprensibile per un avversario. Un sistema di cifratura che tutti abbiamo usato da ragazzi, consiste nel tradurre un testo spostando l'alfabeto di un certo numero di lettere. Se sposto l'alfabeto di tre lettere A diventa C e così via.
Nella crittografia convenzionale si utilizza un algoritmo di cifratura, che è generalmente conosciuto – lo spostamento delle lettere –, e una chiave di cifratura che deve essere concordata ed utilizzata in modo segreto tra due parti – di quante lettere è lo spostamento –.
L'utilizzo di questa tecnica è però problematica su Internet, perché le esigenze di comunicazione non sono predefinite, ma basa su contatti occasionali tra diversi interlocutori. Per questo, anche definendo un algoritmo comune, sarebbe difficilmente pensare a un'attività di scambio delle chiavi tra gli interlocutori perché le possibili combinazioni potrebbero crescere esponenzialmente.
La soluzione a questi problemi è data dalla crittografia a chiave pubblica. La società RSA Data Security all'inizio degli anni '80 ha sviluppato un algoritmo basato su tecniche matematiche sofisticate, che si presta per l'utilizzo su Internet.
L'algoritmo RSA si basa su una coppia di chiavi complementari: una chiave, utilizzata per cifrare, che deve essere obbligatoriamente resa pubblica e una chiave utilizzata per decifrare, che deve essere mantenuta rigorosamente segreta e quindi privata.
Per inviare un messaggio protetto a qualcuno, basta ottenere la sua chiave pubblica e utilizzarla per cifrare, sicuri che il destinatario sarà in grado di decifrarlo con la propria chiave privata. In questo modo la crittografia a chiave pubblica garantisce una comunicazione protetta e riservata dei dati senza concordare nessuno scambio delle chiavi.
Questo algoritmo basato su due chiavi permette anche la firma digitale, garantendo sia l'autenticità del messaggio elettronico sia l'identificazione di chi lo ha inviato. Qui le chiavi sono utilizzate in modo inverso. Per firmare un messaggio il titolare lo cifra con la sua chiave privata. Chiunque è in grado di verificare l'autenticità del messaggio se riesce a decifrarlo con la chiave pubblica del mittente.
Data l'importanza della chiave pubblica, è necessario avere la certezza che essa appartenga veramente al titolare che la dichiara come sua, e non a un impostore che potrebbe utilizzarla per compiere attività fraudolente.
L'Autorità di Certificazione è la società che – simile a un notaio – garantisce, tramite l'emissione di un Certificato Digitale, l'autenticità della chiave pubblica e l'associazione con il titolare.
Queste tecniche permettono alle organizzazioni che forniscono servizi su Internet di dare agli utenti le massime garanzie di sicurezza. Quando un sito utilizza un certificato digitale, è possibile fornire con tranquillità il proprio numero della carta di credito, effettuare transazioni bancarie o come nel caso del recente censimento, inviare dati personali senza il rischio di confrontarsi con degli impostori e soprattutto con la certezza che le informazioni sono inviate in modo protetto.
La crittografia a chiave pubblica è utilizzabile anche da parte degli utenti, istallando un certificato digitale nel proprio browser Web. Questo permette loro di identificarsi con una maggiore sicurezza presso i siti web che accettano questo sistema, evitando l'uso di password, di per se più insicure e scomode da utilizzare. E naturalmente diventa possibile anche per gli utenti inviare messaggi e documenti firmati digitalmente, con tutte le garanzie di integrità del documento e autenticità del mittente. Questa firma digitale, che rende un documento elettronico sicuro come uno firmato in modo autografo, apre nuove prospettive nella corrispondenza ufficiale tra privati, aziende ad enti pubblici su Internet. Per questo il

Dipartimento federale di giustizia e polizia ha messo in consultazione un avanprogetto sulla firma digitale, con lo scopo di recepire le nuove opportunità tecnologiche e fissare nella legge l'equivalenza della firma digitale alla firma autografa.

Solo una convenzione internazionale globale ci difenderà dagli abusi

Incontro con Bertil Cottier, dell'Istituto svizzero di diritto comparato e docente all'USI

Come può la legislazione confrontarsi con le nuove situazioni create dalle innovazioni tecnologiche? Come possiamo continuare a sentirci tutelati nelle nuove realtà globali?
Ne abbiamo parlato con Bertil Cottier , direttore supplente dell'Istituto svizzero di diritto comparato di Losanna, docente presso l'Università della Svizzera italiana, autore di numerosi saggi relativi al diritto comparato e membro di varie commissioni per la redazione di leggi e per l'elaborazione di strumenti internazionali nel campo dei media.

I rapidi cambiamenti delle tecnologie possono essere difficili da seguire da parte del legislatore. In particolare come si può operare in assenza di leggi specifiche su problematiche che coinvolgono aspetti nuovi quali Internet?

Il progresso tecnologico molto rapido è una sfida per il legislatore che è abituato a lavorare in un ambiente stabile e prevedibile. D'altra parte la lentezza del processo legislativo è il prezzo da pagare per un sistema democratico: gli avanprogetti di legge sono prima messi in consultazione presso partici politici, ambienti economici, associazioni, in seguito il parlamento s'incarica di discutere tutti i dettagli dei progetti e alla fine esiste ancora la possibilità di un referendum. Oggi al legislatore, non solo è richiesto di fare più in fretta, ma spesso non ha la certezza dell'efficacia delle soluzioni giuridiche porposte. Questa urgenza e questa incertezza lo costringono ad utilizzare nuovi strumenti legislativi: leggi sperimentali, messa in vigore anticipata di regolamenti di applicazione (progetti semplici di regolamenti di applicazione sono dichiarati applicabili prima della loro approvazione formale), concessioni di assegni in bianco nei confronti dell'amministrazione (ad esempio l'articolo 7 della legge federale sulle telecomunicazioni che rovescia le regole sulla separazione dei poteri permettendo all'autorità concessionaria di stabilire nuove regole se le circostanze dovessero cambiare repentinamente). Per ora questi strumenti permettono di rimediare alle necessità più urgenti, ma se dovessero generalizzarsi, il nostro sistema democratico ne soffrirebbe.

Internet ha caratteristiche nuove, quali la rapidità di comunicazione e la capacità di superare i confini nazionali. Questo significa che siamo di fronte anche alla possibilità di nuovi reati che fino ad oggi non abbiamo conosciuto? Con quali strumenti giuridici si possono combattere?
In effetti i nuovi delitti sono poco numerosi, se per nuovi delitti si intendono quelli che non esistevano prima dell'arrivo dell'autostrada dell'informazione e che non sono una semplice variante "tecnologicamente moderna" di delitti già esistenti.
Per questi nuovi delitti - come il flooding, che consiste nel bombardare una casella postale elettronica di e-mail per paralizzare il sistema informatico – è necessario che il legislatore intervenga adottando le norme repressive necessarie. Per gli altri è possibile utilizzare il diritto esistente; per esempio non c'è bisogno di adottare norme speciali per sanzionare il framing – la creazione di un collegamento ipertestuale verso un sito di una terza persona facendolo passare per proprio – si possono utilizzare le regole che sanzionano il parassitismo, contenuto nella legge sulla concorrenza sleale.
Bisogna dire che il principale problema di Internet resta la sua natura globale che complica gli aspetti di repressione come mai fino ad ora. La sola soluzione veramente efficace è una convenzione internazionale che definisca degli standards comuni a tutti i paesi del globo. Fino ad ora esiste un consenso globale solo per quanto riguarda la repressione della pornografia infantile e le violazioni dei diritti di autore; per tutto il resto i punti di vista divergono da un paese all'altro. Di tutto questo ne approfittano i delinquenti che agiscono a partire dai paesi più permissivi.

Nell'attuale società dell'informazione i dati personali devono essere maggiormente protetti da chi può farne un uso illecito, soprattutto se raccolti tramite Internet fuori dai confini nazionali. Quali sono i punti di vista sulla protezione dei dati

personali a livello internazionale, e che cosa si sta facendo dal punto di vista giuridico a livello transnazionale?

Tutte le legislazioni europee sulla protezione dei dati – compresa la legge federale svizzera – contengono un articolo che proibisce il trasferimento di dati personali in paesi che non hanno un livello di protezione dei dati equivalente agli standard europei (che sono i più elevati al mondo). Queste norme fanno nascere un problema importante con gli Stati Uniti che non sono dotati di una legislazione sulla protezione dei dati degna di questo nome. La soluzione – per non ostacolare le transazioni commerciali elettroniche tra Europa e Stati Uniti – è stata quella di costringere, per mezzo di negoziati difficili e lunghi, le principali aziende americane che operano nei due continenti, ad adottare dei codici di comportamento che assicurano alle persone schedate garanzie analoghe a quelle di cui beneficiano in Europa (diritto di consultare i dati raccolti, diritto di rettificare i dati falsi o non corretti, ecc). In tutti i casi questa soluzione non è la migliore; anche qui, come in tutti i settori toccati da Internet, sarà necessario pensare prima o poi ad una convenzione globale.

La firma digitale è una delle tecniche informatiche che è stata recepita con maggior rapidità dal legislatore, forse per le sue connotazioni e le sue ricadute sul piano giuridico. Quale è la situazione oggi in Svizzera e nel resto del mondo?

In Svizzera il legislatore si accinge a preparare il terreno per una ufficializzazione della firma digitale ; un avanprogetto di legge,allo studio da parte del Dipartimento federale di giustizia e polizia, è stato recentemente messo in consultazione. Oltre a questo, dal mese di aprile 2000 un ordinanza sperimentale regola un aspetto particolare della problematica: i servizi di certificazione. A livello europeo, una direttiva sulla firma digitale è stata adottata nel dicembre 1999; i quindici Stati membri hanno tempo fino al luglio 2001 per emettere le corrispondenti norme nazionali. Alcuni Stati, come l'Italia e la Germania, hanno già dato valore probatorio alla firma digitale.