Internet e ansia di sicurezza: il rischio informatico

Giovanni Pascuzzi

UNA CARATTERISTICA DELL'ERA DIGITALE: L'ANSIA DI SICUREZZA

Il diritto dell'era digitale sembra caratterizzato dall'ansia di sicurezza **[1]**. Senza sistemi informatici sicuri, il diritto alla protezione dei dati personali si svuoterebbe di significato. Sicura si vuole sia la navigazione in rete, specie per scongiurare il pericolo che i minori abbiano accesso a contenuti nocivi o indecenti. Sicuri devono essere i meccanismi di firma, perché alla loro affidabilità è ancorata la certezza dei traffici. Sicure non possono che essere le transazioni sulla rete (si veda il tema dei protocolli per i pagamenti via rete), se il commercio elettronico deve definitivamente decollare.

SICUREZZA E PROTEZIONE DEI DATI PERSONALI

Nel considerando n. 46 della Direttiva 95/46/CE (tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) si legge: "la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere".

Muovendo da quanto prescritto nella sezione VIII della direttiva 95/46/CE, il codice della privacy (d. lgs. 30 giugno 2003 n. 196) impone veri e propri obblighi di sicurezza in capo al titolare del trattamento. In particolare l'art. 31 prevede che i dati personali debbano essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L' Allegato B al codice della privacy contiene il disciplinare tecnico in materia di misure minime di sicurezza. È bene sottolineare che la violazione dell'obbligo di adottare le misure minime di sicurezza (delineate nell'articolo 33 del codice della privacy) è sanzionato penalmente (cfr. art. 169 D. Lgs. 196/2003). Sul piano civilistico, il trattamento dei dati personali è considerato esercizio di attività pericolosa. Infatti, a norma dell'art. 15 del codice appena citato, chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 che elenca i principi in tema di modalità del trattamento dei dati e requisiti dei medesimi.

Alla diffusione sempre più capillare dei computer fa eco una crescente ansia di sicurezza. Tale ansia è alimentata dalla consapevolezza della:

- a. possibile utilizzazione maliziosa e dannosa dei dati personali che riguardano gli individui (e i soggetti diversi dalle persone fisiche);
- b. dipendenza sempre maggiore delle società avanzate dai sistemi informatici e telematici: nel considerando n. 1 del Regolamento (CE) n. 460/2004 si legge: "Le reti di comunicazione e i sistemi di informazione sono ormai fattori determinanti dello sviluppo economico e sociale. Computer e reti stanno diventando strumenti altrettanto comuni dell'acqua corrente o dell'energia elettrica. La sicurezza delle reti di comunicazione e dei sistemi di informazione, in particolare la loro disponibilità, diventa di conseguenza sempre più importante per la società anche a causa della possibilità che si presentino problemi nei sistemi chiave d'informazione a motivo della complessità del sistema, di incidenti, errori e

attacchi che possono avere conseguenze sulle infrastrutture fisiche che forniscono servizi essenziali per il benessere dei cittadini dell'UE" **[2]**;

- c. vulnerabilità dei sistemi: si veda il considerando n.2 del Regolamento appena citato su cui si tornerà più avanti quando si parlerà di sicurezza e commercio elettronico.

SICUREZZA E DOCUMENTAZIONE

Le nuove tecnologie possono essere utilizzate dall'ordinamento per perseguire finalità tradizionalmente perseguite con altre tecnologie (es.: certezza delle relazioni giuridiche). Si pensi al documento elettronico e alla firma digitale, che grazie a regole all'uopo introdotte (cfr., per il nostro Paese, l'iter che ha portato alla emanazione del Decreto Legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale" **[3]**), perseguono le finalità un tempo assicurate da documento cartaceo e sottoscrizione autografa.

Ebbene, anche per il documento informatico rileva il profilo della sicurezza. A norma, ad esempio, dell'art. 21 del Codice dell'amministrazione digitale: "Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza".

SICUREZZA E SOTTOSCRIZIONE

Anche per la firma elettronica si attinge al parametro della sicurezza, specie quando si vuole che la stessa riceva pieno riconoscimento da parte dell'ordinamento in vista del prodursi in capo al titolare degli effetti di volta in volta voluti.

La firma elettronica qualificata (di cui la firma digitale è un esempio) deve essere realizzata mediante un dispositivo sicuro (cfr. art. 1, comma 1, lett r del Codice dell'Amministrazione Digitale). In particolare, a norma dell'art. 35 del citato d. lgs. 82/2005, "I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

- a) sia riservata;
- b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
- c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi".

SICUREZZA E COMMERCIO ELETTRONICO

Nel considerando n. 2 del Regolamento (CE) n. 460/2004 si legge: "Il numero crescente di violazioni della sicurezza ha già provocato notevoli danni economici, turbato la fiducia degli utenti e danneggiato lo sviluppo del commercio elettronico. Gli individui, le amministrazioni pubbliche e le imprese hanno reagito dotandosi di tecnologie e procedure di gestione relative alla sicurezza. Gli Stati membri hanno preso a loro volta numerose misure di sostegno per accrescere la sicurezza delle reti e dell'informazione nella società, come ad esempio campagne di informazione e progetti di ricerca" **[4]**.

Nella seconda metà degli anni '90, con l'esplosione del World Wide Web, la rete diventa strumento per vendere beni e servizi vecchi e nuovi (commercio elettronico). Ci si rende conto che il decollo di siffatte attività sulla rete può essere seriamente ostacolato se i potenziali clienti dovessero sentirsi minacciati da imprecisati rischi. Proprio per accrescere la fiducia dei consumatori nel commercio elettronico, l'Unione Europea ha varato il progetto e-confidence **[5]**.

La sicurezza nel commercio elettronico significa poter essere certi dell'identità dei soggetti che prestano servizi sulla rete (cfr. art. 7 del d. lgs. 70/2003 **[6]**); ovvero che tali soggetti trattino in maniera leale i dati personali in cui si imbattono nell'espletamento della propria attività **[7]**; e così via.

SICUREZZA E PAGAMENTI TELEMATICI

Inutile dire che la sicurezza del commercio elettronico riposa anche sulla sicurezza dei pagamenti che avvengono sulla rete. L'utilizzo di mezzi di pagamento via Internet come contropartita della vendita di beni e fornitura di servizi on line presuppone l'esistenza di una infrastruttura tecnologica avanzata e, soprattutto, sicura. Si pensi, a tale proposito, ai protocolli SET (Secure Electronic Transaction) e SSL (Secure Socket Layer). È necessario, inoltre, scongiurare i rischi di frodi, gioco d'azzardo, pratiche di riciclaggio. In argomento si veda la Decisione quadro del Consiglio dell'Unione Europea (2001/413/GAI) del 28 maggio 2001 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti **[8]**, nonché la Direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo **[9]**.

IL RISCHIO INFORMATICO

Il tema della sicurezza informatica è molto sentito **[10]**. A livello europeo è stata istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004). L'Agenzia ha il compito di contribuire ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nella Comunità e a sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno.

L'art. 4, comma 1, lett. c) del Regolamento (CE) n. 460/20 definisce "sicurezza delle reti e dell'informazione": la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema.

Nel considerando n. 19 del Regolamento si legge: "I problemi di sicurezza delle reti e dell'informazione sono questioni globali. Occorre una maggiore cooperazione a livello mondiale per migliorare le norme di sicurezza, migliorare l'informazione e promuovere un approccio globale comune alle questioni legate alla sicurezza delle reti e dell'informazione, contribuendo in tal modo allo sviluppo di una cultura in materia di sicurezza delle reti e dell'informazione.

Una cooperazione efficace con i paesi terzi e con la comunità mondiale è ormai un dovere anche a livello europeo. A tal fine l'Agenzia dovrebbe contribuire agli sforzi comunitari in materia di cooperazione con i paesi terzi e, se del caso, con organizzazioni internazionali".

In argomento si vedano anche:

- la Risoluzione del Consiglio del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione **[11]**;
- le Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione. Verso una cultura della sicurezza (luglio 2002) **[12]**;
- la Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro);
- la Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni).

La sicurezza informatica può essere messa in pericolo da eventi quali:

- 1. Interruzione o mancanza di servizio (dovuti ad esempio: a catastrofi naturali quali inondazioni o terremoti; incendi; danni fisici alle strutture);
- 2. Fallimento tecnico del sistema (dovuto, ad esempio, a malfunzionamento dell'hardware, alla mancata entrata in funzione dei sistemi di back up, ovvero ad errori di programmazione);

- 3. Distruzione, manipolazione o perdita di programmi e dati per eventi diversi da criminalità informatica;
- 4. Sabotaggio e accesso non autorizzato da parte di dipendenti infedeli;
- 5. Criminalità informatica tesa all'accesso non autorizzato ovvero alla introduzione di virus, worms, back doors, etc.;

Gli eventi appena ricordati possono produrre una varietà di tipologia di danno:

- 1. Manipolazione dei siti web;
- 2. Corruzione e perdita di dati;
- 3. Violazione di database con connessa violazione di dati personali;
- 4. Furto di identità;
- 5. Frodi finanziarie ed economiche (come avviene quando ci si impossessa illecitamente dei numeri di carte di credito);
- 6. Violazione di segreti industriali;
- 7. Perdita di profitti;
- 8. Investimenti per ricostruire l'immagine delle aziende i cui sistemi di sicurezza informatica sono stati violati;
- 9. Investimenti per ripristinare le apparecchiature e il software.

IL PRINCIPIO DI PRECAUZIONE NELL'ERA DIGITALE ... LA PREVENZIONE DEL RISCHIO INFORMATICO AFFIDATA A TECNOLOGIE EVOLUTE: IL TRUSTED COMPUTING

Il rischio informatico può essere affrontato in modi diversi. Sul piano legislativo: nelle pagine che precedono sono state ricordate le numerose disposizioni che si occupano di sicurezza informatica. Sul piano contrattuale: sono sempre più diffuse, ad esempio, le polizze assicurative tese a coprire il patrimonio informatico e le relative responsabilità.

Esiste anche un approccio diverso: è la stessa tecnologia che può apprestare gli strumenti più idonei a garantire la sicurezza informatica. Conviene approfondire quest'ultima alternativa.

L'approccio tradizionale al rischio informatico si sostanzia nella produzione di strumenti software (antivirus, antispyware e firewall) di reazione ad attacchi ai sistemi informatici ed utilizzi impropri dei computer e delle reti Di recente si sta affermando un approccio del tutto innovativo alla prevenzione del rischio informatico: il Trusted computing **[13]**.

"Trusted Computing" (TC) è una delle molteplici espressioni usate per denominare il coordinamento di alcune iniziative che fanno capo ad imprese leader del settore dell'hardware e del software. Il Trusted Computing Group (TCG) è un'organizzazione no-profit promossa da grandi imprese del settore dell'informatica **[14]**.

Nella presentazione sul sito web di riferimento si legge che gli obiettivi del gruppo sono lo sviluppo e la diffusione di specifiche per standard aperti finalizzati alla produzione di sistemi con architettura "Trusted Computing" composta da elementi hardware e software in grado di essere incorporati su differenti piattaforme, periferiche e dispositivi quali personal computer, palmari e telefoni digitali.

Una tale architettura informatica risponderebbe principalmente all'esigenza di rendere più sicuri - ovvero protetti tanto da attacchi compiuti mediante software quanto da attacchi compiuti direttamente sul sistema hardware - la conservazione dei dati, le prassi del business on-line, ed i contratti del commercio elettronico, garantendo la funzionalità del sistema, la privacy ed i diritti individuali. Il TC si basa su un uso massiccio della crittografia. L'attuale concezione del TC risponde, infatti, all'obiettivo di creare un ambiente informatico fatto di hardware e software "sicuro", cioè con caratteristiche diverse da quelle di tutti gli altri sistemi informatici.

Non è un caso che il TC sia destinato ad essere innervato nelle componenti hardware (un microchip della scheda madre) e software (il sistema operativo) basilari **[15]**, in quanto è proprio l'integrazione tra protezioni hardware e software che - come già accennato - garantisce i massimi livelli di protezione tecnologica attualmente possibili. L'aspetto più significativo della logica del TC sta

proprio nella necessità che l'hardware, il software ed i dati dell'utente siano certificati attraverso chiavi crittografiche.

Si pone, dunque, il problema della dislocazione del controllo del sistema informativo dall'utente al certificatore **[16]** (a ben vedere si passa dal controllo sull'informazione digitale al controllo sulle infrastrutture). Il TC si presenta dunque come un approccio assolutamente innovativo alla sicurezza informatica.

L'obiettivo non è quello di produrre nuovi strumenti software (come antivirus, antispyware e firewall) di reazione ad attacchi ai sistemi informatici ed utilizzi impropri dei computer o delle reti, ma al contrario di promuovere la costruzione di sistemi hardware e software non abilitati a determinate funzioni potenzialmente in grado di comprometterne la sicurezza, nonché il controllo - attraverso Internet - del rispetto delle limitazioni di funzionalità da parte degli utenti dei sistemi.

La logica sottesa al TC è quella del "prevenire è meglio che punire". Un sistema è sicuro o affidabile se il suo hardware ed il suo software sono concepiti e costruiti in modo da essere costretti a funzionare nel modo voluto dai produttori e non dagli utenti finali. Ciò comporta almeno due conseguenze: da un lato, la limitazione preventiva delle funzionalità del sistema informatico; dall'altro la dislocazione del controllo del sistema informatico dall'utente finale a chi produce l'hardware ed il software, nonché a chi è deputato a sorvegliare che siano rispettate le limitazioni di funzionalità imposte dal produttore. Inutile dire che chiunque controlli l'infrastruttura TC acquisterà un potere considerevole.

E non è difficile immaginare i tanti modi nei quali sarebbe possibile abusare di tale potere. Inoltre, l'approccio TC alla sicurezza informatica pone due problemi di fondo che sono assai rilevanti sul piano giuridico:

- a. il processo di elaborazione degli standard tecnologici dell'architettura TC così come la gestione della sicurezza sui cui si basa il TC è nelle mani di privati i quali non necessariamente procedono in base a processi trasparenti o democratici;
- b. la sicurezza dipende dall'architettura informatica la quale incorpora non diversamente dalle architetture fisiche alcune regole implicite le quali sono rigide, predeterminate e potenzialmente infallibili **[17]**.

ALCUNI POSSIBILI SCENARI

Il Trusted Computing risponde ad una delle possibili visioni della sicurezza informatica cioè alla logica della "Prevenzione del rischio informatico". Ad un prezzo: quello della "limitazione preventiva delle funzionalità" e della "dislocazione del controllo del sistema informatico dall'utente ad altri soggetti". Il Trusted Computing sta emergendo come architettura della sicurezza per la prossima generazione di PC.

Non è ancora lo standard dominante, ma lo diventerà - con tutta probabilità - nel prossimo futuro. La minaccia alla privacy sta nelle scelte di fondo: limitazione preventiva delle funzionalità e dislocazione del controllo del sistema informatico. Nel caso del TC la decisione - pur giustificabile in base a molte argomentazioni - dello Stato (o degli Stati) di non ingerirsi direttamente nel processo di standardizzazione delle tecnologie di sicurezza può avere effetti collaterali negativi. L'adesione all'architettura TC - e dunque ai valori che essa incorpora - potrebbe diventare nel prossimo futuro un prerequisito per l'accesso alla società dell'informazione.

Le assicurazioni sul rischio informatico potrebbero essere portate a rafforzare lo standard di fatto. Potrebbero ad esempio rifiutarsi di assicurare le (o potrebbero pretendere polizze esose dalle) imprese che decidono di rifiutare di implementare gli standard TC nei propri sistemi informativi. Un'ultima notazione. Nella discussione classica sul principio di precauzione in ambito non digitale si discute di come gestire il gap di informazioni ex ante rispetto all'evoluzione tecnologica ed al rischio che essa produce (di qui la difficoltà di definire ed applicare il principio della precauzione e di misurare quanto e quale diritto statale deve regolamentare lo stesso principio).

Nel diritto dell'era digitale, dove forse si può disporre di tecnologie che prevengono perfettamente buona parte dei rischi, lasciare la precauzione solo ai privati - intesi come centri di potere normativo privato - implica la certezza che alcuni margini di libertà siano sacrificati. Sotto tale profilo l'incertezza, l'elasticità e la fallibilità del diritto possono avere una valenza positiva **[18]**. L'ansia, anche quella di sicurezza, in genere non è una buona cosa se supera la soglia di accettabilità. Il rischio fa parte della vita ed è ineluttabile anche quando nascono nuove tecnologie che lo moltiplicano o che lo riducono.

NOTE

[1] Più in dettaglio per i temi trattati nel presente paragrafo, v.: PASCUZZI, Il diritto dell'era digitale, Bologna, 2006, passim.

[2] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[3] PASCUZZI, Il diritto dell'era digitale, cit., 75 ss.

[4] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[5] Sul punto v.: COMMISSIONE DELL'UNIONE EUROPEA, Consumer confidence in E-Commerce: lessons learned from the E-Confidence initiative Brussels, 8 novembre 2004, SEC(2004) 1390, http://europa.eu.int/comm/consumers/cons_int/ecommerce/ e-conf_working_doc.pdf.

[6] Si tratta del Decreto che ha dato attuazione nel nostro Paese alla Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[7] Un ruolo importante nella traiettoria tesa ad avere siti web sicuri può essere giocato da soggetti terzi che si assumono il compito di garantire che i siti si adeguino a precisi standard concedendo ad essi un marchio di qualità. La direttiva 2000/31 sul commercio elettronico invita le associazioni commerciali, professionali e dei consumatori a contribuire all'elaborazione di un quadro affidabile e flessibile per il commercio elettronico definendo codici di condotta. Molto spesso tali codici sono associati ai cosiddetti trustmark schemes (marchi di fiducia) o labels (marchi di qualità garantita). Per quel che riguarda l'Italia, esempio di questo approccio è il certificato Qweb, servizio fornito da IQNET per il tramite di numerosi enti certificatori tra cui RINA e ICQ. Scopo del marchio di qualità è accrescere la fiducia degli acquirenti nei confronti del commercio elettronico, attestando che il fornitore on-line certificato si attiene a determinati principi e criteri nel condurre operazioni commerciali. Il citato marchio Qweb attesta che: il sito è sicuro e registrato legalmente; il servizio di e-business è della migliore qualità; le condizioni di vendita e di consegna sono chiare e veritiere; la sicurezza e la privacy sono applicate per il trattamento dei dati personali; i reclami del cliente sono presi in considerazione e opportunamente gestiti; i consumatori possono ricorrere a una soluzione extragiudiziale delle controversie.

[8] In Gazzetta ufficiale dell'Unione Europea n. L 149 del 2 giugno 2001. V. anche la prima (SEC(2004) 532 - COM/2004/0346 def.) e la seconda (SEC(2006) 188 - COM/2006/0065 def.) Relazione della Commissione fondate sull'articolo 14 della decisione quadro 28 maggio 2001.

[9] In Gazzetta ufficiale dell'Unione Europea n. L 309 del 25 novembre 2005.

[10] A riprova della accresciuta sensibilità al tema, si può segnalare il fatto che nel nostro ordinamento universitario sta per essere introdotta una laurea magistrale in 'Sicurezza informatica'. Nello schema di decreto relativo alle classi magistrale (elaborato ai sensi del D.M. 270/2004 e relativi allegati, trasmessi al CUN con nota prot.n.Gab/7859.8.1 del 12.9.2006, alla CRUI con nota prot.n. GAB/7860.8.1 e al CNSU con nota prot.n. GAB/7861.8.1 del 12.9.2006) è

prevista infatti la classe della laurea magistrale LM 66, intitolata, appunto, Laurea magistrale in Sicurezza informatica. I laureati magistrali nei corsi di laurea della classe devono:

- conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti;
- conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali;
- conoscere gli aspetti relativi alla organizzazione del lavoro ed alle problematiche di carattere psicologico e sociale come elementi critici rispetto alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici, nonché gli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici e quelli bio-sanitari e bio-etici relativi alle tecniche biometriche ed al trattamento, conservazione e trasmissione dei dati sensibili riguardanti la salute.

[11] 11 GU C 48 del 28 febbraio 2003.

[12] Rinvenibile al sito http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf? OpenDatabase

[13] Diffusamente sull'argomento v.: CASO, Un 'rapporto di minoranza': elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, in CASO (a cura di), Sicurezza informatica. Regole e prassi, Trento, 2006, 5 ss.

[14] V. il sito web: https://www.trustedcomputinggroup.org.

[15] Per una spiegazione della logica alla base dell'architettura del trusted computing v., in senso critico, ANDERSON, 'Trusted Computing' Frequently Asked Questions, versione 1.1. 2003 (agosto), disponibile all'URL: http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html. Il problema si pone anche per i sistemi di DRM, Digital Rights Management. In argomento v., nella letteratura italiana, CASO, Digital rights management ' Il commercio delle informazioni digitali tra contratto e diritto d'autore, Padova, 2004 (ristampa digitale, Trento, 2006, scaricabile dal sito http://www.jus.unitn.it/users/caso/pubblicazioni/drm/hom e.asp?cod=roberto.caso)

[16] V. le critiche di ANDERSON, 'Trusted Computing' FAQ, cit.

[17] Cfr. CASO, Un 'rapporto di minoranza': elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, cit.

[18] Cfr., ancora, CASO, Un 'rapporto di minoranza': elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, cit.