Sicurezza dei pagamenti e privacy nell'e-commerce

Versione 1.0 – aprile 2008

Paolo Guarda

Sicurezza dei pagamenti e privacy nell'e-commerce

Versione 1.0 aprile 2008

Paolo Guarda[*]

1. Le tecnologie digitali ed il loro impatto sulla società

Lo sviluppo delle tecnologie digitali e la sempre maggiore diffusione di Internet inducono sensibili mutamenti nella società e nel comportamento degli individui[1].

Lo sviluppo dell'attività commerciale on-line ed il crescente interesse da parte degli utilizzatori verso gli strumenti offerti dalla rete assumono una rilevante importanza sia da un punto di vista economico che da un punto di vista sociologico: il terreno su cui si gioca il futuro ed il successo della diffusione dell'e-commerce è la positiva o negativa reazione dei singoli, analizzata in maniera aggregata[2].

Vi è una generalizzata paura del nuovo, di ciò che ancora non si conosce e non si comprende del tutto, ed infatti fattori psicologici, quali la diffidenza e la sfiducia, rappresentano importanti ostacoli all'avvicinamento ai mercati elettronici da parte di nuovi utilizzatori.

---

[*] Ripubblicazione inalterata di un articolo già pubblicato in *Diritto dell'Internet*, 2005, 91-101. Questa versione 1.0 – aprile 2008 in pdf -

[1] V. G. PASCUZZI, *Il diritto fra tomi e bit*, Padova, 1997; dello stesso autore, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002.

[2] Per approfondimenti v. C. ABBATE, S. MERCURI, *E-commerce: sicurezza telematica, carte di credito e cybercrimini*, in *Tributi*, 2000, fasc. 10, 1225; D. FORTE, *La sicurezza: gestione di un incidente informatico*, in R. GUIDOTTI, G. ZICCARDI, *Il diritto nell'era di internet*, Modena, 2001, 121-136; B. MACKLIN, *E-commerce at what Price. Privacy Protection in the 'Information Economy'*, paper reperibile su <<http://www.eprivacy.com.au/download/Take4.pdf>>, 8-10; G. FIENGO, *I codici di condotta per il commercio elettronico*, in *Diritto e Formazione*, 2002, 1207; T. T. REITH, *Consumer confidence: the keyto successful e-commerce in the Global market-place*, 24 *Suffolk Transnat'l L. Rev.* 467 (2001). Con specifico riferimento alla sicurezza nei trasferimenti nelle aste on-line e sul contrastato rapporto tra on-line auction e privacy, v. D.E. SORKIN, *Payment Methods for Consumer-to-Consumer Online Transactions*, 35 *Akron L. Rev.* 1 (2001); R.R. DU, K. JAMAL, S. SUNDER, *Control and Assurance in E-Commerce: Privacy, Integrity, and Security at e-Bay*, *Yale ICF Working Paper No. 02-38*, reperibile su <<http://ssrn.com/>>.

Poiché l'acquirente, in un contesto digitale, non può avere un contatto diretto col prodotto, costruire la necessaria fiducia circa la bontà e l'affidabilità dell'attività svolta diviene compito principale per chiunque intenda porre in essere un'attività commerciale on-line.

L'e-commerce si può definire come l'attività di vendita e di acquisto di beni e servizi svolta con l'ausilio e tramite sistemi di comunicazione informatica[3]. In base alle modalità di svolgimento della stessa, occorre distinguere tra le operazioni che riguardano beni e prodotti che possono essere acquisiti dall'utente in via immediata e diretta, con il semplice "scaricamento" da un sito Web previo pagamento del prezzo stabilito (esempio può essere l'acquisto di prodotti musicali in formato MP3), dalle operazioni che necessitano comunque di forme di consegna che potremo definire "tradizionali" o che quantomeno prevedono una non contestualità tra acquisto e consegna. Nel primo caso solo l'utilizzazione di sistemi di pagamento che assicurino un rapido accertamento della solvibilità dell'avente causa e che garantiscano un elevato grado di sicurezza delle conseguenti operazioni finanziarie giustificano e, quindi, favoriscono l'assunzione da parte dell'imprenditore del rischio di impresa per via telematica. Nel secondo caso, la gestione di una parte del rapporto contrattuale con modalità off-line rende lo schema operativo, per vari aspetti, facilmente assimilabile alle forme di operazioni commerciali "ordinarie".

Sorgono, quindi, rilevanti problemi legati alla sicurezza dei nuovi metodi di pagamento. Il successo dell'e-commerce si basa non solo sulle problematiche classiche del rapporto contrattuale, quali l'identificabilità e la non ripudiabilità della proposta e dell'accettazione debitamente espresse, bensì soprattutto, sulla possibilità di porre in essere trasferimenti patrimoniali per via telematica "sicuri" nell'interesse di chi effettua il pagamento, ma anche di chi offre beni e servizi tramite Internet[4]. L'obiettivo fondamentale in questo ambito è quello di riuscire a fornire non una sicurezza assoluta, irraggiungibile anche nello schema classico, e "reale", degli scambi, bensì un grado di

[3] In argomento v. E.M. TRIPODI, F. SANTORO, S. MISSINEO, *Manuale di commercio elettronico*, Milano, 2000; C. e F. SARZANA, *Profili giuridici del commercio elttronico,* Milano, 1999; R. GAMBERALE, *Le problematiche legali del commercio elettronico*, in *Giur.it*, 2001, 417; A. PALAZZOLO, *Profili giuridici del commercio elettronico*, in *Rass. Giur. energia elettrica*, 2000, fasc. 2-3, 403; R. CLARIZIA, *Il commercio elettronico: gli aspetti giuridici generali e le problematiche contrattuali*, in *Riv. Not.*, 1999, I, 1437; PASCUZZI, *Il diritto dell'era digitale*, cit., 117-140; F. SARZANA, *I contratti di Internet e del commercio elettronico*, Milano, 2000; F. DELFINI, *Il d.p.r. 513/1997 e il contratto telematico*, in *Contratti*, 1998, 293; A.M. GAMBINO, *L'accordo telematico*, Milano, 1997; L. ALBERTINI, *Osservazioni sulla conclusione del contratto tramite computers e sull'accetazione di un'offerta in internet*, in *Giust. Civ.*, 1997, II, 21; R. KALAKOTA, A. WHINSTON, *Electronic Commerce. A Management's Guide*, Reading, 1996; B.B. SOOKMAN, *Electronic Commerce, Internet and the Law: A Survey of the Legal Issues*, 48 *U.N.B. L.J.* 119, 159 (1999).

[4] Interessanti approfondimenti in E. GIANNANTONIO, *Trasferimenti elettronici di fondi e inadempimento*, in *Foro it.*, 1991, V, 423; dello stesso autore, *Trasferimenti elettronici di fondi ed adempimento*, *id.*, 1990, V, 165; F. COSSU, *I pagamenti elettronici*, in *Riv. not.*, 1999, 523; G. OLIVIERI, *La rilevanza del tempo nei sistemi di pagamento*, in *Banca, borsa ecc.*, 2000, I, 161; G. STUMPO, *Il quadro tecnico e normativo di riferimento degli strumenti di pagamento on-line*, in *Dir. comm. int.*, 2001, 685; S. MARTUCCELLI, *Obbligazioni pecuniarie e pagamento virtuale*, Milano, 1998; G. DI BENEDETTO, *Anatocismo "eventuale" nell'"appuramento del conto" e nei pagamenti elettronici*, in *Riv. dir. priv.*, 2001, 285-306.

sicurezza relativa che risulti competitivo o, quantomeno, equivalente a quella ottenibile nel commercio per via tradizionale.

Lo sviluppo di nuovi ed alternativi sistemi di pagamento effettuati per via telematica obbliga il giurista ad un ripensamento della teorica classica relativa alle modalità di adempimento dell'obbligazione pecuniaria: la questione coinvolge il più generale fenomeno di dematerializzazione degli strumenti di pagamento emblematicamente rappresentato dallo sviluppo della cd. e-money[5].

Un'altra delle principali problematiche connesse al commercio elettronico è quella relativa alla tutela della privacy delle parti coinvolte nei pagamenti on-line, nonché della sicurezza dei dati personali richiesti al fine di eseguire le varie operazioni negoziali e, più in generale, dei dati che viaggiano sulla rete[6]. La regolamentazione dei rapporti che intercorrono tra gli operatori delle reti telematiche nel momento della loro utilizzazione è un punto fondamentale per uno sviluppo equilibrato del settore. Occorre, poi, tener presente che Internet non ha solo una dimensione visibile. Esiste, infatti, anche un gran numero di trattamenti che avvengono del tutto all'insaputa dell'individuo. Si pensi, ad esempio, ai problemi connessi all'utilizzo dei cookie[7]: questi sono piccolissimi file creati sui computer dai siti che vengono visitati e che consentono ai siti stessi, ogniqualvolta ci si riconnetta ad essi, di riconoscere l'utente. Ove si tratti di garantire la continuità del servizio (pensiamo alla possibilità di non dover digitare la password ad ogni accesso) ovviamente il loro utilizzo risulta legittimo. Essi possono essere utilizzati, anche, per scopi molto più minacciosi: è nota la tecnica di spedire e-

[5] V. R. BORRUSO, *La moneta elettronica (Relazione al convegno organizzato dall'Associazione italiana giovani avvocati, dalla Conferenza dei giovani avvocati e dall'European Young Bar Association sul tema: "Cyber law - Problemi giuridici connessi allo sviluppo di Internet", Roma, 9 luglio 199*8), in *Temi Romana*, 2000, fasc. 1 (aprile), 118-122; J.A. DORN, *The Future of Money in the Information Age*, Cato Institute, 1997, trad. it. *Il futuro della moneta*, Milano, 1998; G. PASCUZZI, *Il diritto dell'era digitale*, cit.,, 105-115; A. PERRONE, *La nuova disciplina italiana sulla moneta elettronica: un'introduzione*, in *Studium iuris*, 2003, fasc. 5, 578-585; V. SANTORO, *Appunti sulla moneta elettronica (intervento al Convegno su "Informatica e situazioni giuridiche soggettive", Camogli, 21-23 novembre 1985)*, in *Riv. not*., 1986, I, 879; O. HANCE, S.D. BALZE , *The New Virtual Money: Law and Practice*, Kluwer Law International, The Hague, London, Boston, 1999. Sul tema della moneta più in generale vedi T. ASCARELLI, *Studi giuridici sulla moneta*, Milano, 1952; C. GIANNINI, G.B. PITTALUGA, *Moneta e istituzioni monetarie*, Milano, 2001; B. INZITARI, *La moneta,* in *Tratt. di dir. comm.,* (a cura di) F. GALGANO, vol. VI, Padova, 1983, 4; T. PADOA SCHIOPPA, *La moneta e il sistema dei pagamenti*, Bologna, 1992; S. SANGIORGI, *Pagamento e moneta scritturale*, Torino, 1998; A. TENCATI, *Il pagamento attraverso assegni e carte di credito*, Padova, 2003; L. FARENGA, *La moneta bancaria*, Torino, 1997; G. LEMME, *Moneta scritturale e moneta elettronica*, Torino, 2003; R. D'ORAZIO, *Il quadro giuridico della moneta elettronica*, in *Dir. inf.*, 2004, 191.

[6] V. G. PASCUZZI, *Il diritto dell'era digitale*, cit., 49-70; D. MEMMO, *La privacy informatica: linee di un percorso normativo*, in *Contratto e impr.*, 2000, 1213; I. ROAGNA, *Problemi in tema di documento informatico. Contratto elettronico e firma digitale*, in *Dir. comm. int.*, 1999, 941; J. LITMANN, *Privacy and E-commerce*, 7 *B.U. J. Sci. & Tech. L.* 223 (2001); L. CILLARIO, *Il tecno-controllo telematico. Un problema spiacevolmente rimosso dalla coscienza collettiva*, in *Democrazia e diritto*, 1997, 243; P. B. MAGGS, *Protezione del consumatore su Internet*, in *Resp. civ. prev.*, 1999, 580; C. ABBATE, S. MERCURI, *Sicurezza e Privacy: le due anime del web* , in *Tributi*, 2001, fasc. 4, 234.

[7] V. B. MACKLIN, *E-commerce at what Price. Privacy Protection in the 'Information Economy'*, cit., 15-16; I. FAYENSON, *Coockies Challenge Meanings of Privacy*, 226 *N.Y. L. J.* 1 (2001); M.S. ROTH, *Beware of Coockies: do Marketers that Track a User's On-line Activities Threaten Privacy?*, 23 *The National L. J.* PC1(2001); V. CARIDI, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Dir. inf.*, 2001, 763.

mail non richieste contenenti il collegamento ad un sito web visitando il quale l'ignaro navigatore consegna (naturalmente a sua insaputa) un coockie col proprio indirizzo di posta elettronica e con i dati delle proprie navigazioni in rete, dati che hanno un'elevata importanza sull'attivissimo mercato del marketing diretto e della pubblicità in rete. In generale, tutte le attività svolte su Internet possono essere facilmente "spiate" attraverso l'utilizzo di vari software: i web bug (cimici web), etichette elettroniche che aiutano i siti web e le imprese di pubblicità a tracciare gli spostamenti dei visitatori della rete e che spesso si nascondo all'interno di banner pubblicitari; gli spyware, codici in grado di raccogliere dati ed inviarli al produttore del software oppure a società che si occupano di telemarketing (generalmente informazioni relative a tipologie e licenze del software installato); la cd. Persistence Internet Explorer, tecnologia pensata per ridurre le comunicazioni tra sito web e browser agevolando la navigazione all'utente ed alleggerendo il carico di lavoro del server web ma che fanno ciò archiviando le ricerche effettuate dall'utente sul motore di ricerca; gli adware (software advertising supported), software gratuiti in cui sono inserite pubblicità, di solito banner, che rallentano la navigazione.

In questo scritto analizzeremo i vari sistemi di pagamento che le nuove tecnologie offrono (par. II). Poi si descriveranno i protocolli di sicurezza utilizzati per criptare e rendere difficilmente accessibili a terzi "malintenzionati" le informazioni finanziarie che viaggiano sulla rete (par. III). Si farà un rapido excursus della legislazione di riferimento, anche in ambito penalistico (par. IV). Verrà dato spazio ad un "intermezzo" comparatistico, accennando alle modalità con le quali la problematica inerente la privacy viene affrontata e risolta nella legislazione statunitense (par. V). Infine si svolgeranno alcune riflessioni conclusive circa il necessario trade off tra sicurezza e privacy nel momento in cui si utilizzino nuovi sistemi di pagamento basati su tecnologie informatiche e sul ruolo del legislatore in questo nuovo contesto digitale (par. VI).

2. I sistemi di pagamento on-line

Lo sviluppo del commercio on-line ha come necessaria conseguenza l'implementazione di nuovi sistemi di pagamento che determinano il passaggio dalla banconota cartacea al contante digitale. Questo fenomeno estremizza una delle caratteristiche di Internet, cioè la dematerializzazione degli strumenti reali e giuridici di cui l'uomo si serve nella vita quotidiana[8].

Negli ultimi anni sono stati creati diversi strumenti per i pagamenti in Internet. Molti di questi richiedono l'intervento di una terza parte che funga da intermediario della transazione. A seconda del tipo di strumento utilizzato, l'intermediario può risultare legato da un rapporto contrattuale al compratore, al venditore o ad entrambi[9].

[8] V. M.J. RADIN, *Information Tangibility*, *Stanford Law School. Public law research paper n. 48* (2002), reperibile su <<http://papers.ssrn>>.

[9] V. J.K. WINN, *Clash of the Titans: Regulating the Competion between Established and Emerging Electronic Payment System*, 14 *Berkeley Tech. L.J.* 675, 691-95 (1999); G.E. MAGGS, *Payment Devices and General Principles of Payment Law*, 72 *Notre Dame L. Rev.* 753, 759-763 (1997). Alcuni dei nuovi

I fondamentali vantaggi connessi all'utilizzo dei metodi di pagamento on-line sono rappresentati dalla convenienza e dall'efficienza degli stessi. Alcuni di questi "caricano" una commissione comparabile a quella che viene addebitata con l'utilizzo delle carte di credito, ma altri sono meno costosi, quando non completamente gratuiti[10]. Poiché i pagamenti on-line restano per molti aspetti non disciplinati, assistiamo ad una sorta di contrattualizzazione dei diritti di compratori e venditori[11].

Le modalità di pagamento utilizzabili nella rete sono sostanzialmente suddividibili in tre gruppi[12].

Innanzitutto, lo strumento sicuramente più utilizzato è rappresentato dalle transazioni che avvengono attraverso l'invio dei dati della carta di credito (cd. sistemi *credit based*)[13]. A dispetto dei tanti dubbi esistenti sulla sicurezza degli acquisti on-line, le carte di credito coprono, secondo gli ultimi dati, l'88% della spesa virtuale mondiale, assicurando un importantissimo beneficio all'e-commerce. Il sistema su cui si basa tale tipo di pagamento è semplice da descrivere: il compratore, dopo aver concluso il contratto on-line, digita sul proprio computer i dati della sua carta di credito che vengono criptati ed inviati al venditore. A seguito di tale invio, il venditore chiederà l'autorizzazione alla propria banca, la quale attraverso il controllo e la verifica dei dati in questione, darà il via all'operazione. I rischi per l'acquirente sono legati alla sicurezza dei dati che viaggiano sulla rete e alla possibilità che questi vengano intercettati e clonati abusivamente da terzi. Il venditore, dal canto suo, non avendo elementi certi sull'identità e sulla reale solvibilità del compratore, corre il rischio di vedersi costretto a restituire l'importo ricevuto, qualora il cliente neghi, in seguito, di aver autorizzato il pagamento. Di particolare importanza in questo ambito è, quindi, l'adozione di sistemi di sicurezza avanzati che garantiscano l'identità e l'idoneità del codice della carta digitato.

Esistono, poi, i cd. sistemi *debit based* che si fondano su meccanismi tipici del sistema bancario. Qui il cliente, dopo aver stipulato una convenzione con la banca ed aver, quindi, aperto un conto corrente on-line, emette a favore del venditore un assegno

---

metodi di pagamento non riguardano direttamente Internet, quali, ad esempio, i sistemi che si basano sull'utilizzo del fax.

[10] Un venditore che desideri accettare i pagamenti con carte di credito può anche dover essere tenuto a sopportare notevoli costi sia iniziali che periodici. I costi da sostenere per le transazioni sono relativamente bassi, ma per i venditori con un basso volume d'affari questi possono apparire proibitivi. Vedi A. ROE, *Merchant Beware: AW's Investigation into Credit Card Merchant Accounts, AuctionWatch.com (Feb. 18, 2000)*, reperibile su <<http://www.auctionwatch.com/awdaily/features/beware/>>.

[11] V. in generale G.E., MAGGS, *Payment Devices and General Principles of Payment Law*, cit..

[12] G. PASCUZZI, *Il diritto dell'era digitale*, cit., 106-110.

[13] Vedi C. PARODI, *Commercio elettronico e tutela penale dei mezzi di pagamento*, in *Dir. pen. e proc.*, 2001, 103, 104-106; C. ABBATE, S. MERCURI, *I sistemi di pagamento...*, cit., 974-975; dello stesso autore., *E-commerce: sicurezza telematica, carte di credito e cybercrimini*, in *Tributi*, 2000, 1225, 1226-1227; P. SPADA, *Carte di credito*, in *Diz. del dir. priv.*, a cura di N. IRTI; G. RESTUCCIA, *La carta di credito come nuovo mezzo di pagamento*, Milano, 1988; A. RIZZIERI, *Carte di credito*, in *Riv. dir. civ.*, 1995, II, 223; P. TRANE, *Le carte di credito*, Milano, 2001; E. PERUSIA, *Carte di credito e dati personali indifesi nel grande far west dell'e-commerce*, in *Dir. e Giusitizia*, fasc. 34, 2000, 73; G. RESTUCCIA, *Le carte di credito nell'ordinamento giuridico italiano,* Milano, 1999; R. BORRUSO, *Gli aspetti legali della sicurezza nell'uso delle carte di credito e di pagamento*, in *Giust. civ.*, II, 217.

che viene convalidato dall'istituto di credito[14]. Il funzionamento in breve è questo: l'acquirente apre un conto corrente on-line; la banca autorizza l'utente ad installare nel proprio hard disk una sorta di libretto di assegni digitale; al momento della transazione l'acquirente appone all'assegno la propria firma digitale e lo spedisce al venditore che, infine, si rivolge all'emittente per incassare la somma.

Troviamo, da ultimo, il cd. sistema *token based*: si tratta di un metodo completamente svincolato dalla fisicità e con rischiosi aspetti di incontrollabilità. La moneta elettronica (in senso stretto, anche detta e-cash) è un valore monetario rappresentato da un credito nei confronti dell'emittente; memorizzato su un dispositivo elettronico dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso; accettato come mezzo di pagamento da imprese diverse dall'emittente[15]. L'introduzione di un mezzo di pagamento assimilabile al contante ripropone la questione relativa all'identificazione della moneta rilevante ex art. 1277 c.c. ai fini dell'adempimento delle obbligazioni pecuniarie[16]. Per altro verso, la circolazione di moneta non emessa dalla banca centrale, ma nel contempo dotata delle medesime caratteristiche proprie del denaro contante, solleva delicate questioni di politica monetaria e di vigilanza.

Si assiste, infine, alla diffusione di un supporto per i pagamenti che offre notevoli vantaggi per la garanzia dell'anonimato e della sicurezza: le smart card. Queste rappresentano, in sostanza, un'evoluzione delle tradizionali carte di pagamento prepagate: a differenza di quest'ultime, che consistono di un supporto laminato su cui è installata una banda magnetica contenente un numero limitato di informazioni, le smart card contengono al loro interno un microprocessore che permette alla carta di memorizzare una quantità di dati notevolmente superiore a quella di una normale carta a banda magnetica[17]. Queste particolari carte si suddividono in due tipi: monouoso, che consentono l'effettuazione di pagamenti nei confronti di un unico soggetto, che spesso coincide con l'emittente; multiuso, che consentono di effettuare pagamenti presso un numero più o meno ampio di esercenti convenzionati. Da quando nel 1989 l'ISO (International standard organization) ha diffuso il documento 7816 (valido in tutto il mondo) riguardante le specifiche tecniche ed il protocollo di comunicazione delle smart

[14] V. PARODI, *Commercio elettronico e tutela penale dei mezzi di pagamento*, cit., 106-107; C. ABBATE, S. MERCURI, *I sistemi di pagamento...*, cit., 975.

[15] Approfondimenti in G. OLIVIERI, *Appunti sulla moneta elettronica*, in *Banca, borsa ecc.*, 2001, I, 809; A. PERRONE, *La nuova disciplina italiana sulla moneta elettronica: un'introduzione*, in *Studium Juris*, fasc. 5, 2003, 578; R. BORRUSO, *La moneta elettronica*, cit.; G. FINOCCHIARO, *Prime riflessioni sulla moneta elettronica*, in *Contratto e impr.*, 2001, 1345; S. CASSESE, *La vigilanza sugli «istituti di moneta elettronica» (commento alla direttiva del parlamento europeo e del Consiglio, 18 settembre 2000, n.2000/46/Ce)*, in *Giornale dir. amm.*, 2001, 186; P. VALENTE, F. ROCCATAGLIA, *La vigilanza sugli «istituti di moneta elettronica» (commento alla direttiva del parlamento europeo e del Consiglio, 18 settembre 2000, n. 2000/46/Ce)*, in *Impresa*, 1999, 1699.

[16] Problema che appare, oramai, superato dalla Direttiva 2000/46/CE.

[17] V. S. NEWMAN, G. SUTTER, *Electronic Payment – the Smart Card*, 18 *Computer L. & Security Report* 307 (2002); J. THEODORE, J. GALATAS, J. SGRO, *A Smart Card Revolution in Payment System*, 76 *Law Institute Journal* 76 (2002); E. ALDER, *Smart Card Technology – Hong Kong*, 18 C*omputer Law & Security Report* 120 (2002); R. CARUSO, *Smart card: le nuove tecnologie al servizio del cittadino*, in *Tributi*, 2001, 320; F. SCOPACASA, *La natura della transazione negli acquisti con smart card*, in *Il Corriere Tributario*, 2002, 2700;

card, ufficialmente queste sono state riconosciute e universalmente definite tanto da far ormai parte del nostro quotidiano. L'implementazione di questo tipo di carte per i pagamenti on-line garantirà un salto di qualità nello sviluppo dell'e-commerce grazie alla loro relativa sicurezza ed agli esigui rischi derivanti da un'illecita clonazione della carta[18].

3. I protocolli per la sicurezza delle transazioni

L'usuale pagamento a mezzo carta di credito, nato negli anni '60, e, quindi, in un'epoca sicuramente antecedente alla diffusione di Internet, è criticato a causa della sua intrinseca pericolosità relativamente al buon fine della transazione. Si teme, infatti, che, allorquando l'acquirente trasmetta al fornitore i propri dati (numero di carta, identità del titolare, scadenza) attraverso Internet, gli stessi possano essere intercettati da terzi ed utilizzati abusivamente. In realtà, il problema sopra esposto potrebbe astrattamente porsi anche al di fuori di Internet, mediante il normale utilizzo della carta di credito: nella ricevuta che rimane in mano al negoziante sono infatti presenti gli estremi della nostra carta di credito.

A differenza di quanto potrebbe sembrare, la parte che, in astratto, corre i rischi maggiori dall'effettuazione di un pagamento a distanza mediante carta di credito è il venditore: questi, infatti, accettando il pagamento senza verificare l'identità tra il titolare della carta di credito e l'acquirente, si trova in una posizione giuridicamente molto debole. L'acquirente, per contro, potrà validamente fruire di una tutela abbastanza forte: potrà proporre azione di nullità del contratto nei confronti del venditore visto che può sostenere, non avendo firmato nulla, di non avere espresso la propria volontà formativa del contratto; potrà, altresì, ottenere dall'istituto di credito emittente il risarcimento della somma fraudolentemente pagata (in forza del disposto di cui all'art 8, co. 2, del d.lgs. 22 maggio 1999, n. 185). La banca, peraltro, non potrà validamente sollevare un'ipotetica responsabilità del titolare per ritardo nella comunicazione di smarrimento, visto e considerato che un uso illecito della propria carta può essere fatto da terzi, anche se il titolare rimane nell'effettiva disponibilità della stessa.

Acquisti falliti, paure sulla sicurezza dei trasferimenti ed insoddisfazione nei confronti degli strumenti utilizzabili sono ostacoli con i quali confrontarsi per garantire lo sviluppo del commercio su Internet. Da qui l'esigenza di implementare standard di sicurezza per le transazioni che avvengono nella rete al fine di costruire la necessaria fiducia tra gli utenti della rete[19].

---

[18] V. L. NEROTTI, *Aspetti giuridici della sicurezza della firma elettronica e delle smart cards*, in *Ciberspazio e diritto*, 2003, 305.

[19] Vedi C. ABBATE, S. MERCURI, *E-commerce: sicurezza telematica...,* cit., 1227; M.R.K. KIPPIN, *Consumer Privacy on the Internet*, 47 *A. F. L. Rev.* 125, 159-160 (1999); L. LAW, S. SABETT, J. SOLINAS, *The Electronic Future of Cash: Essay: How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, 46 *Am. U.L. Rev.* 1131, 1134-1135 (1997); T. W. CASHEL, *Symposium: Financial Services: Security, Privacy, and Encryption*, 3 *B.U. J. Sci. & Tech. L.* 4 (1997); B. MACKLIN, *E-commerce at what Price. Privacy Protection in the 'Information Economy'*, cit., 18-21; R. OPPLIGER, *Security Technologies for the World Wide Web*, Artech House, 2000, 131-170; S. BURNETT, S. PAINE, *RSA Security's Official Guide to Cryptography*, McGraw-Hill, 2001, 227-242; W. STALLINGS, *Cryptography and Network Security, Principles and Practice*, 2° ed., Prentice-Hall, 1999, 441-461.

Un diffuso metodo per garantire i venditori on-line è rappresentato dal protocollo SSL (Secure Sockets Layer)[20], il quale stabilisce un canale di comunicazione sicuro tra un browser ed un server di Internet. Questo protocollo fu implementato da Netscape Communications affinché fosse utilizzato con Netscape Navigator (nacque così la prima versione, la 1.0). La prima versione per il pubblico fu la 2.0 e fu diffusa con Netscape Navigator versioni 1 e 2. Sebbene fosse estremamente ben progettata, le seppur piccole imperfezioni ed i difetti di sicurezza di quest'ultima versione portarono alla rapida evoluzione del SSL version 3.0 nel 1996. Circa nello stesso periodo, la Microsoft Corporation introdusse una tecnologia per la sicurezza del suo nuovo browser Internet Explorer chiamata Private Communication Technology (PCT). La fusione, poi, tra l'SSL e il PCT, al fine di prevedere un'unica proposta per uno standard comune per Internet, portò alla creazione del Transport Layer Security (TLS) protocol.

La componente fondamentale di una connessione protetta dal SSL è rappresentata dal cd. SSL Handshake Protocol: esso comincia con un'obbligatoria autenticazione del server, mentre per il client è opzionale; dopo che il procedimento di autenticazione si è concluso, ha luogo la contrattazione per la sequenza cifrata; il parametro così deciso sarà utilizzato durante l'intera sessione e garantirà la sicurezza di tutti gli scambi di dati.

In un pagamento on-line, quando un consumatore (client) desidera comprare qualcosa su Internet da un commerciante (server) usando una connessione SSL, il procedimento può essere suddiviso in due passaggi: in un primo momento si ha la costituzione della sessione, poi, avviene lo scambio di informazione tra client e server attraverso una connessione sicura[21]. A questo punto, il client può riempire il suo carrello virtuale e quindi pagare il conto. Il client generalmente deve sottoscrivere alcune importanti informazioni personali quali il numero di carta di credito, la data di scadenza, il nome, l'indirizzo per la fattura. Tutte le informazioni che vengono così date in uscita sono cifrate ancora dal server con il protocollo SSL, viene spedita una richiesta per ottenere un punto di transito con conversione dei protocolli (gateway) per il pagamento in Internet e si andrà, così, a chiedere l'autorizzazione alla banca. L'SSL server ottiene, allora, o l'autorizzazione o il rifiuto per la transazione attraverso il gateway per il pagamento, e spedisce il risultato al commerciante ed al consumatore.

Tutto questo, però, non assicura la salvaguardia dei dati della carta di credito una volta che siano stati raccolti dal venditore: se questi non garantisce la protezione dei dati ricevuti, le informazioni inviate dall'utilizzatore non saranno più protette di quanto lo sarebbero state se non fosse stata utilizzata alcuna misura di sicurezza!

Al fine di migliorare la sicurezza dei pagamenti a mezzo carta di credito, nel febbraio 1996 è stato sviluppato uno specifico protocollo denominato SET (Secure

[20] V. B. MACKLIN, *E-commerce at what Price. Privacy Protection in the 'Information Economy'*, cit.,19-20; B. REYES, K. SWAMINATHAN, J. VEGA, Z. YUAN, *Secure Sockets Layer Protocol*, paper reperibile su <<http://www.ece.umd.edu/class/ents650/SSL.pdf>>; R. J. TAKAHASHI, *Server Impact of SSL/TLS Secure Sockets Layer/Transpor Layer Security*, reperibile su <<http://www.corrent.com/pdfs/SSL%20Impact%20White%20Paper.pdf>>.

[21] Mentre la connessione si può definire come un servizio di trasporto, la sessione è un insieme di connessioni con gli stessi parametri criptografici che sono stati negoziati durante l'Handshake.

Electronic Transaction)[22]. Questo sistema garantisce: la confidenzialità delle informazioni trattate; l'integrità dei messaggi; la certificazione di autenticità delle parti coinvolte nella transazione. Esso funziona nel modo seguente: il titolare della carta di credito SET riceve dalla banca emittente un certificato criptato in forza del quale egli è identificato univocamente dall'istituto di credito. Il titolare registra sul suo computer il certificato e, nel momento in cui effettua un pagamento via Internet, dà la possibilità alla banca di certificare al venditore se chi sta utilizzando la carta sia l'effettivo titolare della stessa. Così facendo, la banca si sostituisce al venditore nell'onere di verificare la corrispondenza tra la firma di chi effettua il pagamento e la firma apposta sul retro della carta di credito, onere che, ovviamente, nelle transazioni via Internet, risulterebbe impossibile da assolvere. In questo modo chi riceve il pagamento risulta essere maggiormente garantito visto che, in caso di problemi, potrà tutelarsi sia nei confronti dell'acquirente, che ha negligentemente permesso che altri utilizzassero per lui la carta SET, sia nei confronti dell'istituto emittente che, alla prova dei fatti, non ha saputo garantire un sistema sicuro ed inviolabile. I nuovi contratti delle carte di credito SET imporranno, inoltre, in capo al titolare un rigoroso onere di custodia del certificato. Nel caso in cui si verifichi che qualcuno sia venuto a conoscenza del certificato e del numero della carta di credito, il titolare non può contestare l'eventuale esborso addebitatogli fintantoché non abbia provveduto a denunciare all'istituto di credito emittente la violazione di sicurezza. Il SET, per garantire la confidenzialità delle informazioni, assicurare l'integrità dei messaggi, e autenticare l'identità degli utenti, utilizza la crittografia: sia la cd. Symmetric cryptography (anche conosciuta come Secret key cryptography) che la cd. Asymmetric cryptography (Public key cryptography)[23].

Mettiamo ora a confronto i due protocolli maggiormente diffusi sulla rete per la sicurezza dei pagamenti on-line.

Innanzitutto il SET protegge l'identità di tutte le parti coinvolte nella transazione attraverso la firma digitale; l'SSL non è, invece, predisposto per porre in essere un tale tipo di operazione. Il SET è un protocollo cd. end-to-end, cioè da utente ad utente; il SSL, invece, si dice point-to-point, cioè una connessione da un server ad un client. Il SET, infine, diversamente dal SSL, non solo definisce tutti i necessari protocolli per lo scambio dei dati al fine del trasferimento pecuniario tra il consumatore ed il commerciante, ma anche garantisce che questi dati siano trasferiti alla banca del commerciante. Vi è, però, un'importante difficoltà per lo sviluppo del SET: esso rappresenta una tecnologia nuova, non ancora sufficientemente testata e molto più

[22] V. B. MACKLIN, *E-commerce at what Price. Privacy Protection in the 'Information Economy'*, cit., 20; S. GARFINKEL, G. SPAFFORD, *Web Security, Privacy & Commerce*, O'Reilly, 2002; A. FOURATI, H.K.B.F. KAMOUN, A. BENZEKRI, *A SET Based Approach to Secure the Payment in Mobile Commerce*, paper reperibile su <<http://csdl.computer.org/comp/proceedings/lcn/2002/1591/00/15910136.pdf>>.

[23] La cd. Symmetric cryptography (anche detta Secret Key Cryptograhpy) si basa su algoritmi come il DES attraverso i quali una singola chiave condivisa è usata sia per la criptare che per decriptare i dati. Nella cd. Asymmetric Cryptography (anche detta Public Key Criptography), invece, si utilizza l'algoritmo RSA, col quale colui che spedisce calcola due chiavi che sono matematicamente correlate nel senso che qualsiasi dato in precedenza criptato con con una chiave, potrà essere, poi, decriptato solo con l'altra chiave e viceversa.

difficile da implementare rispetto al SSL: i suoi alti costi, unitamente alla mancanza di incentivi economici per i commercianti, rappresentano un freno alla sua diffusione.

4. La normativa di riferimento

Come spesso accade quando ci si trova a dover dar conto della situazione normativa in riferimento ad un fenomeno nato e diffusosi in Internet, il problema principale è quello dell'adattabilità delle categorie e delle regole tradizionali del diritto ad una realtà rivoluzionaria[24].

LUUnione Europea ha sempre dimostrato di avere consapevolezza della rapida diffusione dei mezzi di pagamento telematici e del loro differente grado di diffusione sul mercato comunitario[25].

La necessità di garantire un'ampia libertà all'evoluzione tecnica dei sistemi di pagamento elettronico, ha portato le istituzioni della Comunità europea all'emanazione, in un primo momento, di una regolamentazione cd. soft: si è preferito cercare di incentivare una sorta di autoregolamentazione della materia da parte degli utilizzatori della rete, riservandosi solo in un secondo momento la possibilità di adottare atti comunitari vincolanti, di recepimento e consolidamento degli standard sviluppatisi nel frattempo.

Soffermandosi sui profili sostanziali degli atti adottati dalla Commissione in tema di strumenti di pagamento elettronici, anzitutto si deve menzionare la raccomandazione dell'8 dicembre 1987, n. 598, che recepisce il Codice di comportamento proposto dalle associazioni bancarie europee in materia di pagamento elettronico. La raccomandazione introduce la definizione di strumento di pagamento virtuale, inteso quale "*operazione di pagamento effettuata tramite una carta a piste magnetiche o incorporate in un microprocessore presso un terminale di pagamento elettronico…*". Si prevede, poi, un regime di ripartizione dei rischi tra le parti, improntato al principio dell'informazione reciproca nella fase esecutiva della prestazione di pagamento ed al principio della limitazione della responsabilità dell'utente-consumatore.

A questo primo atto normativo ha fatto seguito la raccomandazione della Commissione n. 590 del 17 novembre 1988, sui sistemi di pagamento ed in particolare il rapporto tra il proprietario della carta e l'emittente della stessa. Quale aggiornamento, la Commissione ha, poi, adottato il 30 luglio 1997 la raccomandazione n. 489, relativa alle operazioni mediante strumenti di pagamento elettronico, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali sistemi.

Allo sviluppo tecnologico nei vari Stati membri si è risposto con l'introduzione di specifiche norme comunitarie in settori correlati alla cd. contrattazione a distanza ed

[24] V. MARTUCCELLI, *Obbligazioni pecuniarie e pagamento virtuale*, cit.; E. TOSI, *I problemi giuridici di Internet*, Milano, 1999; PASCUZZI, *Il diritto dell'era digitale*, cit., 25-34.

[25] Per approfondimenti v. R. CLARIZIA, *Il commercio elettronico: gli aspetti giuridici generali e le problematiche contrattuali*, cit., 1450-1457; R. D'ORAZIO, *L'azione comunitaria in tema di carte di pagamento*, in *Dir. inf.*, 1988, 958. Sulla sicurezza delle carte di credito in generale, v. BORRUSO, *Gli aspetti legali della sicurezza nell'uso delle carte di credito e di pagamento*, cit.; PARODI, *Commercio elettronico e tutela penale dei mezzi di pagamento*, cit..

alla tutela del consumatore in tale contesto. Si ricordino in proposito, tra le altre, la direttiva n. 85/577/CE del 20 dicembre 1985 in materia di contratti negoziati fuori dei locali commerciali; la direttiva n. 97/7/CE del 20 maggio 1997 riguardante la protezione dei consumatori nei contratti conclusi a distanza; la direttiva n. 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; la direttiva n. 99/93/CE del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche; la direttiva n. 2000/31/CE dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

Tutto ciò ha posto le premesse per l'emanazione di una vera e propria disciplina normativa della materia in esame: la direttiva n. 2000/46/CE, riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività svolta dagli istituti di moneta elettronica (recepita in Italia con la legge comunitaria 1 marzo 2002, n. 39). Questa viene definita come "*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia: memorizzato su un dispositivo elettronico, emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso, accettato come mezzo di pagamento da imprese diverse dall'emittente*". L'emissione è riservata soltanto agli enti creditizi ed agli istituti di moneta elettronica. Il principio cardine è quello della rimborsabilità.

Scopo della direttiva sembra essere quello di introdurre nel mercato unico un nuovo strumento di pagamento, al contempo mirando a garantire un'ampia tutela al soggetto detentore dello stesso.

Nel nostro ordinamento, il quadro normativo di riferimento è costituito dagli artt. 1188 c.c. e seguenti, dall'art. 1277 c.c. e seguenti, nonché dalle disposizioni previste nelle leggi speciali collegate al codice civile in materia di pagamenti alternativi alla moneta avente corso legale ed in materia di pagamento a mezzo di assegno e di cambiale (vedi r.d. 14 dicembre 1933, n. 1669, "Modificazioni alle norme sulla cambiale e sul vaglia cambiario"; r.d. 21 dicembre 1933, n. 1736, "Disposizioni sull'assegno bancario, sull'assegno circolare e su alcuni titoli speciali dell'Istituto di emissione, del Banco di Napoli e del Banco di Sicilia"; l. 15 dicembre 1990, n. 386, "Nuova disciplina sanzionatoria degli assegni bancari". Ai sensi dell'art. 1277, comma 1, c.c., i debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale[26]; l'art. 1197, comma 1, dispone, poi, che il debitore non possa liberarsi eseguendo una prestazione diversa da quella dovuta anche se di valore uguale o maggiore, salvo che il creditore vi consenta. Problemi sono, allora, sorti in ordine alla possibilità di operare un'equiparazione tra la moneta elettronica e quella tradizionale, e circa la conciliabilità degli strumenti di pagamento virtuale con il disposto di cui all'art. 1197 c.c. I dubbi non sono stati del tutto fugati dall'introduzione del d.lgs. 22 maggio 1999, n. 185, recante le norme di attuazione in materia di contratti a distanza: con specifico riferimento alle modalità di pagamento, infatti, il decreto contempla espressamente la possibilità che esso venga effettuato a

[26] I dubbi sorti in dottrina sulla possibilità di considerare la moneta digitale come moneta avente corso legale ai sensi dell'art. 1277, co. 1, c.c., sono, oramai, stati risolti dalla direttiva 2000/46/CE che ha espressamente previsto la valenza e l'utilizzabilità di tale sistema di pagamento.

mezzo di carta di credito, ove ciò sia previsto tra le modalità di pagamento da comunicare al consumatore, prevedendo anche che, nel caso in cui il pagamento risulti effettuato in eccesso rispetto al prezzo pattuito, ovvero sia frutto di un uso fraudolento della carta da parte del fornitore o di un terzo, il consumatore, fatta comunque salva l'applicazione della normativa vigente in materia di riciclaggio, abbia diritto ad ottenere il riaccredito della somma da parte dell'istituto di emissione, il quale a sua volta avrà titolo a rivalersi direttamente sul fornitore, per le somme riaccreditate al correntista.

Dopo questo rapido excursus sulla normativa in materia di pagamenti telematici, è forse opportuno dar conto, almeno per cenni, di alcuni aspetti penalistici di cui si connota il tema in oggetto.

Il continuo diffondersi di Internet solleva diverse questioni in riferimento alla responsabilità dei crimini informatici commessi per mezzo o a danno della rete: ricorrono le varie fattispecie criminose dell'accesso abusivo a terminali e banche dati, la diffusione di virus, la diffusione di materiale illecito[27].

In Italia, la legge 23 dicembre 1993, n. 547 (modifiche ed integrazioni al codice penale in materia di criminalità informatica) ha introdotto nel nostro ordinamento una disciplina specifica andando così a colmare un vuoto normativo[28]. Rinveniamo allora nel nostro codice penale il reato di cui all'art. 615 *ter* c.p. che punisce l'accesso non autorizzato a sistemi informatici o telematici introdotto per la difficoltà concettuale di applicare i reati previsti per il furto dei beni materiali ai beni informatici, non suscettibili ontologicamente di spossessamento o sottrazione[29]. Tale reato è configurabile solo ed esclusivamente nel caso di sistemi informatici o telematici protetti

[27] Per un approfondimento v. A. OLIVA, *La tutela penale del diritto alla privacy in Internet*, in *Riv. pen.*, 2002, 91; G.R. STUMPO, *Internet e privacy: le misure di tutela da adottare per l'utente-consumatore*, in *Dir. e pratica società*, 2002, fasc. 1, 38; dello stesso autore, *Privacy e Internet: un connubio ancora difficile*, in *Riv. personale ente locale*, 2001, 53; G. CORASANITI (a cura di), *Codice per l'informatica - Internet, informatica nelle pubbliche amministrazioni, commercio elettronico, firma digitale, tutela del software, privacy, banche dati*, Milano, 2001; C. RESTA, *Tutela della privacy in Internet: quali limiti e quali necessità?*, in *Impresa*, 2001, 958; R. IMPERIALI, R. IMPERIALI, *Internet e privacy: Usa e Italia a confronto*, in *Dir. e pratica società*, 1999, fasc. 8, 36.

[28] Per maggiori chiarimento v. G. PICA, voce *Reati informatici*, in *Dig. Discipl. Pen.*, IV ed., vol. aggiorn., Torino, 2000, 522; dello stesso autore , *Diritto penale delle tecnologie informatiche*, Torino, 1999; L. PICOTTI, voce *Reati informatici*, in *Enc. Giur.*, aggiornamento, VIII, Roma 2000, 1; C. PECORELLA, *Il diritto penale dell'informatica*, Padova, 2000; P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997; M.M. ALMA, C. PERRONI, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. e proc.*, 1997, 504; A. MASI, *Frodi informatiche e attività bancarie*, in *Riv. pen. economia,* 1995, 427; F. PAZIENZA, *In tema di criminalità informatica: art. 4 l. 23 dicembre 1993 n. 547*, in *Riv. it. dir. e proc. pen.*, 1995, 1089; A. ROSSI VANNINI, *La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/93 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. pen. economia*, 1994, 427; M. PETRONE, *Le recenti modifiche del codice penale in tema di documento informatico: problemi e prospettive*, in *Dir. inf.*, 1995, 259.

[29] V. L.D. CERQUA, *Accesso abusivo e frode informatica: l'orientamento della cassazione*, in *Dir. e pratica società*, 2000, fasc. 16, 51; D. LUSITANO, *In tema di accesso abusivo a sistemi informatici o telematici (Nota a Trib. Torino, 4 dicembre 1997, Zara)*, in *Giur. it.*, 1998, 1923; C. PARODI, *Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare*, in *Dir. pen e proc.*, 1998, 1038; M. NUNZIATA, *Il delitto di «accesso abusivo ad un sistema informatico o telematico»*, Bologna, 1996; R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico. Il concetto di domicilio informatico e lo jus excludendi alios (nota a Trib. Rovereto, 2 dicembre 2003)*, in corso di pubblicazione sulla rivista *Dir. pen. proc.*.

da dispositivi di sicurezza: il crimine viene in tal modo limitato al solo caso in cui il titolare del sistema abbia voluto espressamente limitarne l'accesso alle sole persone autorizzate. Ricorrono, poi, il reato di danneggiamento informatico di cui all'art. 635 *bis* c.p. che punisce chiunque distrugga, deteriori o renda, in tutto o in parte, inservibili sistemi informatici o telematici o programmi altrui; l'art. 615 *quinquies* c.p. (diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) che sanziona la condotta di chiunque diffonda, comunichi o consegni un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento; il reato di frode informatica, di cui all'art. 640 *ter* c.p., che comprende ogni alterazione del funzionamento del sistema informatico o telematico o l'intervento senza diritto su su dati, informazioni o programmi contenuti in un sistema informatico o telematico[30]. Rilevanti sono, infine, le fattispecie criminose di cui agli artt. 617 *quater*[31] e 617 *quinquies* riguardanti rispettivamente la fraudolenta intercettazione, impedimento o interruzione di comunicazioni relative a sistemi informatici e telematici, e l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Riguardo, infine, alla creazione di uno standard comune di sicurezza per l'uso dei sistemi crittografici, esistono in Italia solo alcuni scarni riferimenti all'interno di varie disposizioni normative.

Merita sola menzione la legge 15 marzo 1997, n. 59, che all'art. 15 dispone che "*al fine della realizzazione della rete unitaria delle pubbliche amministrazioni, l'Autorità per l'informatica nella pubblica amministrazione è incaricata, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, di stipulare, nel rispetto delle vigenti norme in materia di scelta del contraente, uno o più contratti-quadro con cui i prestatori dei servizi e delle forniture relativi al trasporto dei dati e all'interoperabilità si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite*". Al secondo comma dello stesso articolo si legge "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*". I criteri e le modalità di applicazione sono stati previsti con successivi specifici regolamenti, tra i quali il d.p.r. 10 novembre 1997, n. 513, (regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della L. 15 marzo 1997, n. 59) in cui si rinvengono le prime nozioni fondamentali per il

[30] V. S. GRECO, *La frode informatica*, in *Temi romana*, 2000, 505; C. PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Dir. pen. e proc.*, 1997, 1538; A. DELLO IACOVO, *Art. 640 ter: truffa o furto? la frode informatica e il «modello 640»*, in *Temi romana,* 1996, 597.

[31] V. C. PARODI, *Detenzione abusiva di codici d'accesso a sistemi e illecito impedimento di comunicazioni telematiche*, in *Dir. pen. e proc.*, 1998, 1149.

nostro ordinamento, tra le quali la definizione del concetto di crittografia a chiavi asimmetriche[32].

5. Intermezzo comparatistico: mezzi di pagamento on-line e privacy nella normativa statunitense

Il commercio elettronico, malgrado le sue enormi potenzialità è stato rallentato ed ostacolato da un'onnipresente paura che alcuni nascosti "criminali" informatici fossero pronti a rubare importanti informazioni, relative agli strumenti di pagamento che si stanno utilizzando, fornite dal consumatore stesso all'atto di acquistare degli articoli nel mercato virtuale[33]. Molti autori sostengono, infatti, che i progressi della moneta elettronica siano fondamentali per garantire la sicurezza e per trasformare Internet in un mercato virtuale mondiale[34].

Poiché ogni pagamento on-line si determina attraverso uno scambio di dati, i rischi per la sicurezza che si possono presentare sono vari e diversi[35]: vi sono quelli strettamente legati alla privacy dell'utente che attraverso le sue operazioni lascia nella rete "tracce" riguardanti i suoi gusti ed i suoi interessi commerciali; vi sono i rischi legati alla gestione delle banche dati che raccolgono tali informazioni; vi sono i pericoli legati alla possibile intercettazione delle comunicazioni da parte di terzi interessati alla utilizzazione abusiva dei mezzi di pagamento di altri[36]; vi è, infine, la necessità che le agenzie governative adibite alla lotta alla criminalità e alla difesa pubblica siano messe nella situazione di poter operare e tracciare anche in Internet le operazioni dei sospetti criminali[37].

---

[32] Art. 1, lettere d) e) f), in cui si dispone che ai fini del presente regolamento si intende: "*d) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici; e) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica; f) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi*".

La disciplina generale sulla materia dell'informatizzazione si rinviene ora nel d.p.r. 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa -, e sue modificazioni.

[33] V. R.T. MUTH, *Security on the Internet*, 70 *Wisc. L. Rev.* 17, 18 (1997); CASHEL, *Financial Services: Security, Privacy, and Encryption*, cit.; LAW, SABETT, SOLINAS, *The Electronic Future of Cash: Essay: How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, cit.

[34] V. C.M. DOWNEY, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, 14 *J. Mashall J. Computer & Info. L.* 303 (1996).

[35] V. T.W. CASHEL, *Symposium: Financial Services: Security, Privacy, and Encryption*, cit.; C.M. DOWNEY, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, cit.; B.S. SCHULTZ, *Comments: Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 *U. Cin. L. Rev.* 779 (1999).

[36] V. G.W. LORENZ, *The Electronic Future of Cash: Essay: Electronic stored value payment systems, Market Position, and Regulatory Issues*, 46 *Am. U.L. Rev.* 1177 (1997).

[37] V. A. DAVIDSON, *Increasing Security without Decreasing Privacy and Freedom*, *Law Rev. Mich. St. U.-Det. C.L.* 783 (2002); A. GIDARI, *Balancing Open Access and National Security Goals*, *Law Rev.*

L'esistenza di un'ampia protezione della privacy è fondamentale per favorire gli usi commerciali di Internet, l'impatto economico dei quali non deve essere sottostimato.

A causa di un'evidente incapacità governativa di provvedere ad una normativa realmente efficace, gli utilizzatori di Internet, assieme con i provider, stabiliscono di volta in volta le regole applicabili ai loro rapporti definendo, così, il livello di civiltà, di anonimato, e di pubblicità commerciale ritenuta accettabile[38].

Come risultato di quella che viene definita una "relaxed regulatory structure", Internet è divenuta una comune risorsa di importanza internazionale, che ha portato alla trasformazione-transizione da una sorta di "spazio digitale" ad una comunità globale con i suoi propri valori, standard di condotta, strumenti di disciplina. In assenza di specifiche norme di tutela, le transazioni nella rete effettuate con metodi di pagamento on-line possono divenire oggetto di furti e truffe informatiche[39]. Inoltre, un sistema di pagamento elettronico che fallisca nel prevenire gli accessi non autorizzati alle informazioni personali dell'utente compromette i diritti individuali connessi alla riservatezza dei dati. Solo quando i singoli confideranno nel fatto che la moneta elettronica garantisca un sufficiente livello di sicurezza, Internet potrà veramente sviluppare tutte le sue potenzialità commerciali[40].

Nonostante l'innegabile esigenza di offrire soddisfacenti livelli di sicurezza per proteggere i pagamenti effettuati con moneta elettronica, le leggi applicabili, ed il common law in generale, non risultano idonei a proteggere gli utilizzatori da possibili abusi[41].

Prendiamo ora in considerazione le più importanti disposizioni legislative in materia[42].

Mich. St. U.-Det. C.L. 765 (2002); A. CAVOUKIAN, *Technology Can Ensure Both Privacy and Security*, *Kitchner-Waterloo Rec.*, Jan. 10, 2002, 13.

[38] V. DOWNEY, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, cit., 316.

[39] V. A.M. FROOMKIN, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 *J.L. & Com.*, 395 (1996); L. LAW et AL., *The Electronic Future of Cash: Essay: How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, cit., 1140-42; S.L. LELIEVELD, *How to Regulate Electronic Cash: An Overview of Regulatory Issues and Strategies*, 46 *Am. U. L. Rev.* 1163 (1997).

[40] V J. CHUNG, *The Digital Performance Right in Sound Recordings Act and Its Failure to Address the Issue of Digital Music's New Form of Distribution*, 39 *Ariz. L. Rev.* 1361 (1997); W.A. HODKOWSKI, *Comment, The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 *Santa Clara Computer & High Tech. L.J.* 217, 274 (1997); M.A. FIXLER, *Note, Cyberfinance: Regulating Banking on the Internet*, 47 *Case W. Res. L. Rev.* 81, 108 (1996).

[41] Anche i tradizionali privacy tort non prevedono strumenti di tutela per i possibili danni alla riservatezza che presenta il diffondersi dell'uso di strumenti di pagamento elettronici, almeno non nella quadripartizione proposta dal Prof. Prosser: Restatement (Second) of Torts 652B (1977). George B. Trubow parla, infatti, di una nuova "information privacy" che rende la suddivisione proposta non utilizzabile per i problemi che si presentano in Internet: G.B. TRUBOW, *The Development and Status of Information Privacy Law and Policy in the United States, Invited Papers on Privacu Law: Law, Ethics, and Technology 1*, raccolta di paper presentati al National Symposium on Personal Privacy and Information Technology, Oct. 4-7, 1981; v. anche S. SIMITIS, *Reviewing Privacy in an Information Society,* 135 *U. Pa. L. Rev.* 707 (1987).

[42] Non prendiamo in considerazione la legge che, invece, riguarda direttamente la materia dei trasferimenti monetari on-line perché non direttamente collegata all'intercettazione e all'accesso non autorizzato a dati finanziari: l'Electronic Fund Transfer Act (EFTA) del 1978. Per un approfondimento v. D.L. POINTER, *The Electronic Fund Transfer Act: an Effective Shield and a Sharp Sword!*, *Amry Lawyer*

Il Privacy Act del 1974[43] è stata la prima legge federale che abbia riconosciuto la necessità di un bilanciamento tra gli interessi individuali relativi alla privacy informatica e la pratica delle pubbliche amministrazioni di raccogliere le informazioni in banche dati computerizzate[44]. Questo statute disciplina appunto l'attività di gestione dei dati da parte delle pubbliche amministrazioni: ogni agenzia federale deve registrare tutte le sue banche dati presso il cd. Federal Register e, con alcune eccezioni, i dati non possono essere trasmessi ad alcun'altra persona o agenzia governativa senza la richiesta od il consenso scritto dell'interessato. Inoltre, il Privacy Act permette all'interessato di copiare, correggere e cambiare i propri dati personali raccolti presso la banca dati.

In teoria questa legge limita la possibilità da parte della pubblica amministrazione di collezionare ed usare tutti i dati personali. Di fatto, comunque, il Privacy Act è una legge scarsamente applicata in quanto presenta numerose eccezioni che limitano grandemente il suo impatto pratico[45]. Queste eccezioni, assieme ad un linguaggio assai vago ed indefinito, permettono alle agenzie governative di schivare tutte le azioni legali promosse da privati cittadini[46]. Oltre alla sottolineata assenza di un'adeguata tutela contro gli abusi posti in essere dalla pubblica amministrazione, il Privacy Act è carente anche dal punto di vista della tutela nei confronti dei privati, non essendo disciplinata la gestione dei dati da parte di questi. La legge non prevede alcun tipo di tutela contro la divulgazione non autorizzata a terzi dell'identità degli utilizzatori della moneta digitale, della loro situazione finanziaria e dei loro interessi commerciali. Più in particolare, non proibisce l'accesso non autorizzato alle informazioni finanziarie raccolte in un database computerizzato o l'intercettazione di tali tipo di dati che passano dall'utilizzatore di moneta digitale ed il venditore.

In conclusione, il Privacy Act non solo non alcuna protezione contro gli abusi della pubblica amministrazione, ma anche, e soprattutto, non tutela contro le iniziative illecite di terzi privati.

Il Financial Privacy Act 1982 (RFPA)[47] è stato emanato per predisporre una più efficace garanzie per le informazioni finanziarie[48]. Il suo scopo specifico è quello di

---

3 (1990); L. S. ADAMS, D.J. MARTZ, *Developments in Stored-value Cards and Cyberbanking*, 54 *Business Lawyer* 1373 (1999); J. MARCUCCI, *The Brave new World of Banking on the Internet: the Revolution of our Banking Practices*, 23 *Nova L. Rev.* 739 (1999); L.L. HEVES III, N.S. PRESTON, *Is there a Time Bomb in Electronic Fund Trasnfer Act?*, 100 *Banking L.J.* 274 (1983).

[43] 5 U.S.C. 552a (1976).

[44] In generale v. C.M. DOWNEY, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, cit., 309-311; J.A. GLADSTONE, *Essay: Technology, the Law, and a Changing World in the Twenty-first Century does the EC Council Directive NO. 95/46/EC Mandate the Use of Anonymous Digital Currency?*, 22 *Fordham Int'l L.J.* 1907, 1916 (1999); M. FINKIN, *Information Technology and Workers' Privacy: The United States Law*, 23 *Comparative Labor Law & Policy Journal* 471 (2002).

[45] V. E. HENDRICKS ET AL., *Your Right to Privacy: A Basic Guide to Legal Rights in an Information Society*, 2d ed., 1990, 8.

[46] V. G.M. KALOW, *Note, From the Internet to Court: Exercising Jurisdiction over World Wide Web Communications*, 65 *Fordham L. Rev.* 2241 (1997); C.L. WILSON, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 *Creighton L. Rev.* 671 (1997).

[47] 12 U.S.C. 3401-3422 (1994).

[48] V. GLADSTONE, *Essay: Technology, the Law, and a Changing World in the Twenty-first Century does the EC Council Directive NO. 95/46/EC Mandate the Use of Anonymous Digital Currency?*, cit., 1915-1916; S.A.J. EISENBERG, *The Right to Financial Privacy Act the Eagle Peeks behind the Veil*, 119 *Banking L.J.* 608 (2002); R.E. BROOKS, *The Financial Privacy Act and the Sovereign Immunity*, 113

bilanciare l'interesse dei privati consumatori alla protezione dei propri dati bancari con l'interesse pubblico all'applicazione della legge. Per raggiungere questo obiettivo, il RFPA non costringe colui che è sottoposto ad un'investigazione a dare volontariamente alle agenzie governative l'accesso ai propri dati. Per ottenere i dati finanziari del consumatore da una istituzione bancaria, il governo deve seguire la procedura richiesta nella legge in oggetto e sottoscrivere una certificazione[49]; occorre, poi, notificare al consumatore un subpoena assieme ad un avviso in cui si ricorda che i documenti registrati sono rilevanti per una "legitimate law enforcement"[50] e che esso può sempre attivarsi per bloccare la divulgazione da parte della banca[51].

Anche se il RFPA ha esteso la protezione della privacy, esso, comunque, soffre di molti dei difetti del Privacy Act. Come questo, infatti, si applica solo a soggetti pubblici, e, quindi, non garantisce un'adeguata tutela nei confronti di abusi perpetrati da soggetti privati. Nulla impedisce a chi gestisce un database di divulgare informazioni personali riguardanti dati finanziari a società commerciali o a "criminali" informatici. Oltre a ciò, lo statute in oggetto non prevede nemmeno una protezione così approfondita nei confronti degli abusi perpetrati da parte di pubbliche amministrazioni: per esempio, se le agenzie governative sospettano che una persona usi Internet per riciclare del denaro (elettronico), possono obbligarla alla rivelazione delle sue informazioni finanziarie semplicemente affermando che tali informazioni sono indispensabili e rilevanti per una "legitimate law enforcement inquiry". Tutto questo rende palese il fatto che il Financial Privacy Act non garantisce una protezione sostanziale della privacy, prevedendo più semplicemente procedure flessibili attraverso le quali le informazioni finanziarie possono essere ottenuti.

L'Electronic Communications Privacy Act (ECPA)[52] del 1986 protegge, invece, gli individui contro l'intercettazione non autorizzata di comunicazioni elettroniche[53]. I Title I e II dell'ECPA si riferiscono alle comuni comunicazioni computer-to-computer, che includono le trasmissioni di dati bancari o trasferimenti di fondi tra istituti

---

Banking L.J. 271 (1996); M.C. HUTTON, *The Right to Financial Privacy Act: Tool to Investigate Fraud and Discover Fruits of Wrongdoing*, *Army Lawyer* 10 (1983).

[49] Section 3403(b) RFPA: "*a financial istitution shall not release the financial records of a customer until the Governement authority seeking such records certifies in writing to the financial institution that it has complid with the applicable provisions of this chapter*".

[50] 12 U.S.C. 3401(8) dove la "*law enforcement inquiry*" viene definita come una "*lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant thereto*".

[51] Cosa tra l'altro non così semplice e di rapida efficacia.

[52] 18 U.S.C. 2510-2518. L'ECPA fu emanato nel 1986 per emendare il Title III of the Omnibus Crime Control Safe Streets Act, che autorizzava l'attività di intercettazione telefonica con i c.d. "Title III warrants". L'ECPA protegge contro l'accesso non autorizzato, l'intercettazione, o la divulgazione di comunicazioni private ed è diviso in due parti: il Title I pone vincoli alle intercettazioni orali, telefoniche, e alle comunicazione elettroniche mentre esse avvengono ("in transit"), mentre il Title II si riferisce all'acquisizione e alla divulgazione di comunicazioni già registrate. V. S.E. GINDIN, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 *South Dakota L. Rev.* 1153 (1997); J. J. MCMURRY, *Privacy in the Information Age: the Need for Clarity in the ECPA*, 28 *Wash. U. L. Q.* 597 (2000); D. HUENEMAN, *Privacy on Federal Civilian Computer Networks: a Fourth Amendment Analysis of the Federal Instrusion Detection Network*, 18 *J. Marshall J. Computer & Info. L.* 1049 (2000).

[53] L'ECPA definisce comunicazione elettronica "*any trasnfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire ... that affects interstate or foreign commerce ...*", 18 U.S.C. 2510(12).

finanziari. Il Title I riguarda direttamente le intercettazioni di comunicazioni via cavo, orali ed elettroniche. Il Title II si riferice all'accesso di dati registrati, inerenti a comunicazioni o transazioni elettroniche: esso statutisce esplicitamente che un provider "*shall not knowingly divulge the contents of a communication while in electonic storage*"[54], quando le comunicazioni arrivano elettronicamente ed il service provider conserva i dati solo per il trattamento e l'archiviazione.

Tra gli statute sopra analizzati, l'Electronic Communications Privacy Act è quello che prevede la più alta forma di protezione dei dati: esso infatti estende la tutela nei confronti di taluni soggetti privati e regola l'accesso alle informazioni trasmesse e archiviate. Tuttavia, nonostante la sua (proclamata) ratio, l'ECPA offre una limitata protezione all'utilizzatore di moneta digitale. Anche se, infatti, come abbiamo già visto, questo statute regola l'accesso ai dati registrati, tale proibizione è applicabile solo alle intercettazioni di trasferimenti finanziari. Inoltre, non proibisce che il gestore del database intercetti, utilizzi, o divulghi una particolare comunicazione elettronica, se lo ritiene necessario per proteggere i diritti del fornitore della moneta elettronica[55].

Sebbene, quindi, questa disposizione normativa preveda alcune tutele per la privacy dell'utilizzatore dei metodi di pagamento on-line, la mancanza di criteri oggettivi per valutare quando l'accesso ai dati finanziari sia necessario presta il fianco a diversi tipi di abusi[56].

L'insufficienza della normativa esistente richiede probabilmente l'emanazione di una legge federale ad hoc che affronti direttamente queste problematiche. Tale nuovo statute dovrebbe adattarsi alla realtà del mondo del commercio on-line prevedendo delle chiare linee guida che disciplinino l'attività di coloro che pongono in essere pagamenti elettronici. Senza tutto ciò, Internet non riuscirà a raggiungere il suo vero potenziale in ambito commerciale[57].

6. Conclusioni: privacy e sicurezza nell'e-commerce

Il fatto che lo strumento solutorio per eccellenza di un rapporto obbligatorio, la moneta, subisca un processo di dematerializzazione che viene portato alle estreme conseguenze dallo sviluppo tecnologico obbliga il giurista ad un'attenta riflessione su due concetti che assumono, oramai, nel mondo digitale un'importanza primaria: la privacy, intesa non solo come tutela dei propri dati, ma anche dei propri interessi commerciali, dei propri gusti, in generale di tutte le informazioni che l'utente "lascia" durante la sua navigazione; la sicurezza, definibile come l'esigenza di proteggere l'integrità dei dati che viaggiano sulla rete. La sicurezza può avere tra i suoi obiettivi quello di tutelare la privacy, in quanto non vi è reale controllo dei dati personali senza

[54] 18 U.S.C. 2510.

[55] V. 18 U.S.C. 2511(2)(a)(i).

[56] Inoltre, sebbene l'ECPA garantisca una certa qual forma di protezione nei confronti di comportamenti illeciti di terzi privati, esso ha, però, il grave difetto di prevedere una protezione sostanziale ben inferiore nei confronti delle intercettazioni poste in essere da agenzie governative.

[57] V. D.L. NICEWANDER, *Electronic Banking-Smart Cards*, *Cyberspace and the Internet*, 50 *Consumer Fin. L.Q. Rep.* 22, 26 (1996); R. W. SIFERS, *Note, Regulating Electronic Money in Small-Value Payment Systems: Telecommunications Law as a Regulatory Model*, 49 *Fed. Comm. L.J.* 701, 727-728 (1997).

un adeguato livello di sicurezza, ma può, anche, trovarsi in contrapposizione con essa, quando ad esempio interessi di ordine pubblico e di contrasto alla criminalità impongono l'utilizzo di strumenti estremamente intrusivi[58].

La capacità di rimanere anonimo resta una delle più importanti attrattive per l'utilizzatore di Internet. Nel mondo reale l'anonimato è stato per lungo tempo utilizzato per denunciare la commissione di reati, abusi politici e frodi fiscali, proteggersi dalle sanzioni, o fornire scottanti rivelazioni. Con la sempre maggiore diffusione di software utilizzati dai siti web per "tracciare" i movimenti degli utenti registrandone i comportamenti, la possibilità di rimanere anonimi è diminuita. Attraverso la diffusione dei pagamenti on-line, gli utenti dei vari siti non saranno più in grado di compiere transazioni in maniera anonima, come invece erano soliti fare utilizzando il denaro contante nel mondo reale.

La partita si giocherà, allora, sulla diffusione e sull'implementazione di tecnologie che permetteranno la navigazione e lo svolgimento di operazioni nella rete con modalità meno invasive e meno rischiose per la privacy degli utenti. Con lo spegnersi dell'euforia iniziale che sta contraddistinguendo lo sviluppo di Internet, e con l'acquisizione della consapevolezza della pericolosa intrusività delle varie tecnologie adibite al tracciamento dei comportamenti e degli interessi degli utilizzatori della rete, diverrà necessaria l'adozione di protocolli, di software e di supporti fisici (ad esempio le smart card) che siano in grado di rendere più sicuro e "anonimo" il navigare sulla Rete.

Altra importante implicazione è quella relativa al rapporto-bilanciamento tra la tutela della privacy e la garanzia del buon operare da parte delle istituzioni adibite alla sicurezza pubblica: l'anonimato e la sicurezza delle comunicazioni finanziarie devono essere controbilanciati dalla previsione di efficaci strumenti di lotta alla criminalità che sempre più sfrutta il contesto digitale per svolgere la propria attività illecita.

In conclusione, si registra in Internet una notevole distanza tra il livello di conoscenza e la percezione del fenomeno da parte del legislatore da un lato, e l'esperienza e la perizia che contraddistinguono, dall'altro, gli utilizzatori della rete. Tutto ciò fa ritenere sicuramente più efficiente che la disciplina venga decisa e testata a livello degli utenti di Internet, mentre il legislatore dovrebbe limitarsi ad emanare atti normativi contenenti delle regole guida (cd. soft law)[59]. Probabilmente un intervento normativo particolarmente dettagliato, volto a dare una disciplina esaustiva al fenomeno, avrebbe effetti dannosi e non raggiungerebbe lo scopo di trovare la corretta allocazione tra interessi diversi e, talvolta, confliggenti.

[58] Sul tema del giusto check and balance tra privacy e sicurezza si possono trovare alcuni approfondimenti, soprattutto nella prospettiva di una sempre maggior intrusività dello Stato nella rete dopo gli avvenimenti dell'11 settembre 2001, nel mio scritto *Agenti software e sicurezza informatica*, in G. PASCUZZI (a cura di), *Diritto e tecnologie evolute del commercio elettronico*, Padova, Cedam, 2004, 315-342.

[59] Per un approfondimento, v. F. PARISI, J. KLICK, *Functional Law and Economics: The Search for Value-Neutral Principles of Lawmaking*, 79 *Chicago-Kent L. Rev. (Forthcoming Winter 2004)*, reperibile su <<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=441941>>.