

Nuove forme di commercio: violazioni ed accertamenti

ANTONIO CILLI¹

SOMMARIO: *Premessa - 1. Internet e la rivoluzione del commercio - 2. Il pagamento su Internet con le carte di credito - 3. La giurisprudenza sulle truffe con le carte di credito - 4. I rischi derivanti dal pagamento on-line - 5. Notizie dai gruppi di discussione su Internet - 6. I canali di discussione in tempo reale - 7. Le difficoltà di accertamento delle violazioni - 8. Nota bibliografica - 9. Appendice: 17 diapositive*

PREMESSA

Il Decreto legislativo 114/98 (denominato "Bersani", dal nome del ministro proponente), pubblicato sulla Gazzetta Ufficiale n. 80/L del 24 aprile 1998, contiene la riforma della disciplina relativa al settore del commercio.

Prevede alcune riforme sostanziali sull'esercizio delle attività commerciali. In particolare si prefigge di perseguire le seguenti finalità: l'efficienza, la modernizzazione e lo sviluppo della rete distributiva, nonché l'evoluzione tecnologica dell'offerta.

La novità più interessante per il nostro settore è certamente il riconoscimento normativo, dettato all'art. 21, del "commercio elettronico". La norma prevede che il Ministero dell'industria, del commercio e dell'artigianato promuova l'introduzione e l'uso del commercio elettronico con azioni volte a:

- a) sostenere una crescita equilibrata del mercato elettronico;
- b) tutelare gli interessi dei consumatori;
- c) promuovere lo sviluppo di campagne di informazione ed apprendimento per operatori del settore ed operatori del servizio;

¹ cilli@bmpe.unich.it Docente di informatica presso la facoltà di Economia ambientale dell'Università "G. d'Annunzio" di Chieti. Consulente della Procura di Pescara per le violazioni informatiche e di informatica giuridica. Coautore del testo "Il commercio elettronico" ed. Utet 1999.

- d) predisporre azioni specifiche finalizzate a migliorare la competitività globale delle imprese, con particolare riferimento alle piccole e alle medie, attraverso l'utilizzo del commercio elettronico;
- e) favorire l'uso di strumenti e tecniche di gestione di qualità volte a garantire l'affidabilità degli operatori e ad accrescere la fiducia del consumatore;
- f) garantire la partecipazione italiana al processo di cooperazione e negoziazione europea ed intenzionale per lo sviluppo del commercio elettronico.

In questo senso sono previste convenzioni e accordi di programma tra il Ministero dell'Industria e soggetti pubblici o privati, nonché con associazioni rappresentative delle imprese e dei consumatori.

Prima di fare previsioni ed esaminare i risvolti dell'avvento del "commercio elettronico" è bene guardare lo stato della tecnologia rispetto alle correnti attività commerciali. Sarà utile conoscere l'iter delle violazioni, fino ad ora compiute, per adottare tutti gli accorgimenti tecnici idonei a limitare l'entità del fenomeno.

1. INTERNET E LA RIVOLUZIONE DEL COMMERCIO

Sempre più navigatori di Internet sono attratti - per facilità e celerità dell'operazione - dal fare *shopping* in Rete.

L'opportunità di incontrarsi nei mercati virtuali della Rete ha eliminato le barriere che separavano le imprese dai consumatori ed i venditori dagli acquirenti. Esistono già varie tipologie di beni acquistabili attraverso la Rete: si possono distinguere i beni immateriali - *software* e servizi informativi - da quelli materiali che invece possono essere ordinati tramite i dispositivi elettronici ma che si avvalgono poi di un sistema misto per l'ottenimento del prodotto. Come avviene un acquisto da Internet?

Si comincia dal compilare una *form* con i propri dati e l'indicazione del prodotto desiderato e si finisce con lo scegliere la forma di pagamento più idonea. Sono molti quelli che scelgono di pagare *on-line*: la sola fatica è quella di leggere e trascrivere i numeri.

C'è da dire, però, che coloro che hanno avuto spiacevoli sorprese a riguardo, ci pensano più volte prima di abbandonarsi al piacere di fare l'operazione senza alzarsi dalla propria poltrona.

Ma cominciamo con l'analizzare la validità di un contratto concluso "xxxtramite" la Rete: l'elemento essenziale è la fiducia tra le parti, così che il cliente invia l'ordine, aspettandosi di ricevere dal fornitore l'esatto quantitativo di prodotto ordinato.

Se le parti rispettassero gli accordi, non ci sarebbe sistema più pratico per spostare le attività commerciali nelle reti telematiche! Ma cosa accade quando, per esempio, il quantitativo di merce ordinato non corrisponde a quello ricevuto? Come può l'acquirente dimostrare qual era il quantitativo realmente richiesto? E che dire del venditore per quanto riguarda l'onere della prova sulla qualità e sul prezzo pattuito?

Analizziamo solo alcune operazioni commerciali concluse via *e-mail* e a mezzo *browser*.

È dato per scontato che un contratto concluso tramite Internet o attraverso qualsiasi rete telematica, è prima di ogni altra considerazione un "contratto". Questa affermazione non è così banale come potrebbe apparire dalla semplice lettura. Con questo chiarimento, anche in presenza di diverse legislazioni il contratto produce sempre degli effetti.

2. IL PAGAMENTO SU INTERNET CON LE CARTE DI CREDITO

Vediamo ora di approfondire il fenomeno italiano del pagamento su Internet tramite le carte di credito (American Express, Carta Si, Mastercard, Visa) che rispondono sicuramente all'esigenza di celerità dell'operazione. È il caso di indicare che da qualche anno si sta diffondendo il fenomeno della moneta virtuale *e-money*, considerata la terza generazione dei mezzi di pagamento su Internet. Questo argomento richiede una trattazione a parte per poter considerare il valore giuridico della moneta elettronica.

Indipendentemente dall'esperienza personale, il pagamento tramite l'uso diretto di una carta di credito presenta il problema "rischio" per una serie di circostanze. L'utilizzo di carte di credito senza numero di codice (PIN) è certamente un pericolo concreto. Ma cosa avviene in caso di pirateria e soprattutto chi ne paga le conseguenze?

In questo caso il commerciante non può essere sicuro che il mandante sia effettivamente il titolare della carta, a meno che non vengano utilizzati sistemi di autenticazione riconosciuti validi dalle parti. Diversa è la situazione in caso di smarrimento o furto di carte di credito, utilizzate

poi illecitamente da altre persone. Nonostante la sicurezza che molti sistemi offrono nel criptare i dati trasmessi, il pericolo della pirateria informatica non è da sottovalutare.

Per questo motivo si è fatto ricorso alla nuova figura degli "intermediari elettronici", cioè a un terzo soggetto che, ricevendo l'incarico dall'acquirente, gestisce il pagamento al venditore dopo aver consentito la verifica del suo mandatario.

Il D.P.R. 513/97 (che ha recepito la "Bassanini1") all'art. 14 introduce il "pagamento informatico", cioè il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati secondo le regole tecniche che dovevano essere emanate entro novembre 1998. Il regolamento che attendiamo dovrebbe essere risolutivo anche per i problemi di sicurezza dei dati previsti dall'art. 15 della legge 675/96 - legge sulla tutela dei dati personali - che però ha già partorito il D.P.R. 318/99 in G.U. 14-09/1999 "individuazione delle misure minime di sicurezza". Il citato Regolamento, da una prima lettura, oltre a non fornire indicazioni di carattere "tecnico" e quindi direttamente applicabile, non può essere esaustivo a giudicare dall'entità dei complessivi 10 articoli che lo compongono.

3. LA GIURISPRUDENZA SULLE TRUFFE CON LE CARTE DI CREDITO

Non abbiamo ancora pronunce giurisprudenziali rilevanti sui nuovi casi di violazione attraverso i sistemi elettronici. Possiamo però esaminare alcuni aspetti tipici delle violazioni, attraverso l'utilizzo delle carte di credito tradizionali.

Il Tribunale di Milano nel febbraio del 1994, ha condannato un negoziante per aver omesso di verificare la corrispondenza della firma dell'acquirente dal documento di riconoscimento alla carta di credito. Nella sentenza pubblicata in "Nuova Giurisprudenza Civile, 1995, I, 179" è stata riconosciuta sia la violazione degli obblighi contrattuali che la violazione del principio del *neminem laedere* esteso anche ai rapporti di credito.

Sempre il Tribunale di Milano nel novembre 1992 aveva ritenuto responsabile un negoziante per aver, in un breve lasso di tempo, accettato carte di credito rubate non richiedendo l'autorizzazione dell'emittente,

poiché le singole operazioni non superavano il limite giornaliero di spesa consentita.

Il Tribunale di Pescara nell'ottobre del 1994 ha ritenuto che il reato di possesso e acquisizione di carte di credito di provenienza illecita, previsto dall'art. 12 della L. 197/91, è un reato di pericolo - per la cui consumazione non è richiesta l'effettiva lesione del bene giuridico - e non si richiede che il profitto venga conseguito.

La stessa violazione commessa attraverso la Rete non cambia l'imputazione del reato, ma sicuramente il giudice si troverà di fronte ad accertamenti che possono andare oltre la sua competenza territoriale con tempi ben più lunghi per la definizione del procedimento.

4. I RISCHI DERIVANTI DAL PAGAMENTO ON-LINE

Quando si verifica la pirateria attraverso i sistemi e le reti informatiche la giurisprudenza fa fatica a consolidare i principi appena esposti.

D'altronde, se con l'utilizzo di una carta di credito si può denunciare l'esercente per aver omesso il controllo tra la firma sulla tessera e quella sul documento d'identità, il discorso non è ancora applicabile ad un pagamento in Rete privo di sistemi di sicurezza (ad oggi non obbligatori) e in mancanza dell'uso della firma digitale, introdotta dal citato Regolamento - D.P.R. 513/97 - ma non applicabile per mancanza di ulteriore regolamento tecnico, oltre che di applicazione di quello già emanato.

Passerà alla storia la rivoluzione della carta stampata e delle firme non più apposte con penna e inchiostro, ma rischiamo di far scrivere sui libri di storia che, dopo tanta attesa, c'è stato un periodo d'inerzia per cominciare ad usare i nuovi strumenti tecnologici.

Non dobbiamo illuderci che, con questa normativa, la rivoluzione possa dare i suoi effetti in tempi brevi.

Ma dopo aver raggiunto questo traguardo, tra i primi in Europa, possiamo guardare un attimo al passato. Gli anni 1996-98 sono stati molto importanti per il riconoscimento legislativo dell'evoluzione tecnologica e dell'avvento della rete telematica Internet. Grazie anche alle riforme in tema di semplificazione amministrativa la legge Bassanini, n. 59/97 ha stabilito che: «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 transmis-

sione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge».

Fino ad ottobre '98 la sperimentazione della firma digitale è stata attivata solo in 5 città italiane: Bologna, Modena, Torino, Siena, Pesaro. Eppure le riforme in atto, come quella del commercio elettronico, facevano presagire un interesse collettivo per l'applicazione delle tecnologie di firma digitale nei diversi settori commerciali. Ad esempio, le Pubbliche Amministrazioni dovrebbero cercare nuove forme di collaborazione con le imprese per produrre più servizi ai cittadini.

Il bisogno di questa collaborazione e la ricerca di regole comuni, non è certo solo il problema italiano. L'Unione Europea sta seguendo tutti gli sviluppi tecnologici e in tema di firma digitale ha pubblicato sulla gazzetta del 6 aprile 1999 un parere del Comitato delle regioni in merito alla «Proposta di direttiva del Parlamento europeo e del Consiglio relativa a regolamenti sulle firme elettroniche». Negli obiettivi della proposta si legge che, anche se in molte situazioni è possibile reperire soluzioni soddisfacenti..... malgrado le firme digitali realizzate tramite tecniche crittografiche siano attualmente considerate un importante tipo di firma elettronica, il quadro di regolamentazione europeo deve essere sufficientemente flessibile da includere altre tecniche che possono essere impiegate per garantire l'autenticazione. I problemi non mancheranno, alcuni appaiono prevedibili e quindi evitabili, ma in corso d'opera si dovranno adottare sicuramente tutti gli accorgimenti necessari per consentire lo sviluppo e la fiducia nelle nuove tecnologie da parte di tutti i cittadini.

Ulteriore pericolo, da approfondire con la propria Banca è che alcune carte, utilizzate per più pagamenti che non superano singolarmente il tetto massimo di spesa, obbligano il proprio Istituto a versare tutte le somme - superando il proprio *plafond* mensile - ai Servizi Interbancari che gestiscono le carte. Né potrebbe derivare l'obbligo per il cliente di rimborsare conseguentemente la propria Banca. Non a caso alcune pagine informative, diffuse anche via Internet contengono l'avvertenza "Sconsigliamo l'utilizzo in chiaro del vostro numero di carta su Internet", oppure "I sistemi di sicurezza attualmente in uso non sono pienamente riconosciuti dai circuiti internazionali visa e mastercard/eurocard". La seguente informativa è consultabile al seguente indirizzo Internet: <http://www.cartasi.it/java/istruzioni.html>.

Tornando al discorso rischio del commercio elettronico, in prevalenza legato alla forma di pagamento, la soluzione - almeno per il momento - si deve ricercare nella lettura dei *contratti* stipulati per l'acquisto della propria carta di credito. Il plurale all'affermazione "contratti" non è fortuito, perché esistono almeno 3 contratti: il contratto tra venditore e consumatore, il contratto tra emittente e titolare della carta e il contratto tra emittente e commerciante. Quest'ultimo contratto offre all'Istituto di Credito la possibilità di accreditare dal conto del commerciante anche le eventuali somme contestate dal cliente. Non si tratta dunque di inventare modelli nuovi di rapporti contrattuali o particolari forme di sicurezza nei rapporti commerciali *on-line*. La prevenzione, e soprattutto la chiarezza del contratto, possono evitare spiacevoli sorprese o l'insorgere di un contenzioso con inutili perdite di tempo e denaro.

5. NOTIZIE DAI GRUPPI DI DISCUSSIONE SU INTERNET

Esistono decine di migliaia di gruppi di discussione, sparsi nel mondo, presenti su Internet. Dal 1994 è stata introdotta in Italia la gerarchia *it*, che raccoglie quasi trecento gruppi in lingua italiana. È possibile accedere a questi gruppi, anche in assenza di *software* specifico. Con un *browser* potete cercare l'indirizzo del tipo: <http://www.mailgate.org/mailgate/index.html> ed accedere direttamente ai gruppi di discussioni italiani.

Per esempio nei gruppi *it.discussioni.consumatori.tutela* o *it.discussioni.consumatori.rete* si discutono spesso delle truffe o dei nuovi raggiri perpetrati a danno degli utenti ignari dei rischi delle transazioni in Rete.

Riportiamo di seguito alcuni messaggi per capire il tono delle discussioni:

Subject: Truffe con PagoBancomat - Soldi facili subito!
Date: Wed, 15 Apr. xxxx
* Newsgroups: it.discussioni.consumatori.tutela
* From: xxxxxxxx@iol.it
* Subject: Truffe con PagoBancomat - Soldi facili subito!

Questa vicenda è vera, purtroppo!

Mi arriva a casa l'estratto conto della mia banca (importa quale?), sul quale campeg-

gia nelle informazioni alla clientela il seguente messaggio che riproto integralmente.

Si sono verificate negli ultimi mesi truffe a danno di utilizzatori di sportelli bancomat durante l'operazione di prelievo contante. I malviventi impediscono, con abili manipolazioni, la restituzione della carta al legittimo titolare convincendolo, offrendo la loro collaborazione, a digitare di nuovo il codice segreto in loro presenza. I malviventi riescono in seguito a recuperare le carte dallo sportello bancomat e, conoscendo il codice segreto, effettuando prelievi contante o acquisti POS.

"Per evitare prelievi fraudolenti, occorre prestare la massima attenzione nell'uso e custodia della propria carta evitando di digitare il codice segreto in presenza di estranei.

Nel caso la carta non venisse restituita o si accorgesse di comportamenti anomali, è necessario bloccarla al numero verde 167-822056 o contattare la propria dipendenza.

Ecco, questo è l'avvertimento, ma quanto è attuabile??? Quante volte usiamo il pagobancomat su terminali POS e digitiamo il codice nel mezzo di supermercati o altri esercizi commerciali e di ristorazione, tanto per dire ben tre esempi? Quando sono stati annotati il codice segreto e i riferimenti bancari (ben in vista sul dorso della carta), sono sufficienti per clonare carte bancomat? Mi direte "serve anche il know-how, bisogna sapere cosa scrivere e come scriverlo", ma davvero è un problema?

La storia vera di una mia collega di lavoro è semplicemente questa. martedì 7 aprile si accorge di essere priva del suo fidato bancomat, alla cosa non dà peso, avendolo scordato a casa più volte in passato e quindi credendolo al sicuro. Al venerdì le viene comunicato che il suo conto è in rosso e la tessera bancomat è stata trattenuta da un terminale di prelievo contante. Cade dalle nuvole e scopre che da giovedì 9 fino al momento del ritiro da parte della macchinetta per ben quattro volte è stato prelevato contante e pure effettuati acquisti di una certa consistenza che farebbero pensare a spese del supermercato per entità e le venti-sessanta lire conclusive dell'importo. La mia collega, pur essendo talvolta distratta, è una persona affidabile e mi fido di lei quando dice che potrebbe aver lasciato il tesserino su una macchina di prelievo contante, ma non ha la più pallida idea di come abbiano ottenuto il codice segreto. Una delle ipotesi che abbiamo fatto è che la tessera sia stata raccolta martedì e dopo un paio di giorni sia arrivata in mano ai soliti ignoti che hanno sovrascritto un loro codice segreto su quello originale - ipotesi maledettamente realistica - oppure il bancomat fosse tatocco e abbiano attraverso un falso specchio ritratto la tessera e osservato la digitazione del codice segreto.

Alcuni mesi fa, ormai sono passati degli anni, una banda molto bene organizzata aveva predisposto un "copybancomat" in cui un sottile pannello della misura e aspetto "giusti" veniva sovrapposto al pannello di inserimento della tessera, registrava la traccia magnetica e filmava con una spy-camera il codice segreto. Sarebbe l'unica spiegazione che mi convince, visto che permette la clonazione delle carte, con prelievi garantiti anche al confronto-firma. Per contrastare queste truffe servirebbe un innalzamento del livello di diffidenza nell'uso delle carte sia da parte degli utenti che da parte degli esercenti, non mi scandalizzerei se qualcuno mi chiedesse anche la carta d'identità.

Vengono anche in mente che il tesserino sia stato raccolto e usato - in ultima ipotesi - da personale competente di una qualche banca, solo per il fatto che hanno già "per lavoro" la possibilità di accedere ad apparecchi e archivi usati per codificare le stesse

carte. Mi rendo conto che è come dare dei ladri alla polizia e non è mia intenzione offendere nessuna delle categorie citate, ma essere bancari o poliziotti non può essere automaticamente considerato una patente di onestà e limpidezza

Ragà, state accorti. Se la mia banca mi avvisa che "da alcuni mesi" si stanno verificando questi episodi non si tratta del caso isolato, presumo quindi che ci sia una vera e propria organizzazione che segue questo ramo di attività a delinquere, e forse il sistema migliore per bloccarli subito è tenere sul conto una liquidità minima!!

Perdere in tre giorni mesi e mesi di risparmi. Grazie no!

* Newsgroups: it.discussioni consumatori tutela

* From: xxxx@tin.it

* Subject: Re. Truffe con PagoBancomat - Soldi facili subito!

Il 16 Aprile, xxxx@nowhere.com ha scritto: 3.000.000 in contanti (limite massimo di prelievo mensile con un bancomat... ma ci vorrebbero almeno SEI giorni per riuscire a prelevare 3 milioni!!!!!!) Sicuro??

Una volta lessi su una rivista che le macchine Bancomat non aggiornano in tempo reale il database della banca emittente (se fai prelievi da istituti diversi dal tuo). Addirittura si parlava di aggiornamenti fatti alle 8 di mattina, ma su questo non ci credo molto. Comunque, se è vero che gli aggiornamenti non sono in tempo reale, sarebbe possibile fregare i 3 milioni in poche ore.

Anni fa fu scoperta una truffa basata proprio su questi tempi e su info prelevate da Internet -)

* Newsgroups: it.diritto

* From: xxxxx@tin.it

* Subject: USO ABUSIVO DI CARTA DI CREDITO. RIMEDI?

* Date: 20 Apr xxxx

Ciao a tutti. Leggendo l'ultimo estratto conto della mia Carta Si ho purtroppo constatato che alcune società o soggetti sconosciuti con strani nomi inglesi hanno ottenuto degli accrediti attraverso transazioni su Internet che ovviamente non ho mai fatto.

Si tratta di non elevati importi, per fortuna, con operazioni in dollari. Ho subito protestato con il mio gestore il quale, dopo mille controlli e discussioni, ha detto che provvederà a sostituirmi la carta, ma che non può bloccare più i pagamenti.

Possibile che non ci sia alcun rimedio a situazioni simili?

Chi è responsabile di tali addebiti, se io non ho mai firmato nulla, né autorizzato la società che gestisce la mia Carta a pagare alcunché su ordini via Internet? È sufficiente oggi che chiunque, rubando un numero di carta di credito, possa ricevere delle somme

senza mia autorizzazione e poi sparire nel nulla senza che si possa fare nulla?
Chiedo a voi tutti più esperti lumi su questa situazione che penso possa riguardare tutti gli utenti di Internet

Ringrazio in anticipo chi darà aiuto (anche via *e-mail*)¹

* Newsgroups: it.diritto

* From: studioxxxxx@writeime.com

* Subject: USO ABUSIVO DI CARTA DI CREDITO RIMEDI?

* Date: 20 Apr xxxx

Ciao a tutti. Leggendo l'ultimo estratto conto della mia Carta Si ho purtroppo constatato che alcune società o soggetti sconosciuti con strani nomi inglesi hanno ottenuto degli accrediti attraverso transazioni su Internet che ovviamente non ho mai fatto.

Ho appena scoperto che anche a me è successa la stessa cosa.

Darò battaglia fino in fondo ai Servizi Interbancari (società che gestisce la carta Si), finché non riotterrerò il riaccredito delle somme (fortunatamente basse) illegittimamente sottrattemi.

Non avendo dato alcun ordine di pagamento alla società, credo che le possibilità di successo siano notevoli.

Se sarà necessario coinvolgerò il Comitato difesa consumatori ed eventualmente le varie trasmissioni televisive (Mi manda Raitre o il programma di Lubrano).

Il problema è serio, in quanto le transazioni tramite Internet non hanno alcun tipo di controllo e chiunque può restare fregato, senza che usi la carta in Rete (è sufficiente che un cameriere poco corretto prenda nota del numero di carta e del nome di un qualsiasi cliente di un ristorante, e si diverta poi a fare acquisti in Rete).

Non me ne vogliano i camerieri, l'esempio poteva riferirsi a chiunque, senza voler criminalizzare nessuna categoria.

Comunque, se a qualcun altro è successo qualcosa di simile, propongo di coalizzarci facendo unico fronte contro le società che gestiscono le carte.

Inviatemi pure messaggi in *e-mail* e concorderemo cosa fare.

Non occorrono troppi commenti per capire l'utilità della diffusione delle notizie su canali aperti alle più diverse tipologie di utenti. Su Internet, in particolare attraverso questi gruppi di discussione, sono state smascherate organizzazioni e raggruppamenti che altri mezzi di comunicazione avrebbero fatto fatica a raggiungere.

6. I CANALI DI DISCUSSIONE IN TEMPO REALE (CHAT)

La Rete offre l'opportunità di chiacchierare in tempo reale su argomenti di proprio gradimento. Non esamineremo in questo caso i canali italiani di *chat-line* o meglio IRC - *Internet Relay Chat* -, conosciuti soprattutto dai giovani per particolari tipi di conversazione, ma mi limiterei ad indicare che, nonostante la difficoltà nel reperire una lista ufficiale e stabile di indirizzi, esistono alcuni canali preposti alla discussione di argomenti legati al commercio e alle nuove tecnologie. La ricerca, dunque, di questi canali può avvenire iscrivendosi ad una *mail-list* italiana dedicata a IRC e chiedere ai partecipanti notizie sullo specifico argomento. Un canale dove avvengono discussioni *on-line* delle problematiche con il pagamento su Internet attraverso le carte di credito, è denominato *#carding*.

Il vantaggio di poter chiedere e ricevere informazioni in tempo reale è innegabile. L'unico problema è che di queste conversazioni non rimane - almeno in apparenza ed alla portata di tutti - alcuna traccia scritta. Si è portati a pensare, - per episodi oggetto di indagine - che attraverso queste conversazioni si potrebbero diffondere i numeri di una carta di credito, in modo da utilizzarlo illecitamente nel più breve tempo possibile. Le conseguenze di un'ipotetica condotta sarebbero devastanti per colui che ha subito il furto in virtù delle considerazioni sulle problematiche contrattuali, già esposte, di un carta di credito. Non meno rilevante è la difficoltà tecnica di accertamento di tutte le violazioni, che avvengono attraverso l'uso di strumenti elettronici e soprattutto attraverso le reti telematiche.

7. LE DIFFICOLTÀ DI ACCERTAMENTO DELLE VIOLAZIONI

Il Consiglio dell'Unione Europea ha recentemente formulato una proposta che adotta un Piano pluriennale d'azione comunitaria per promuovere l'uso di Internet - pubblicato in gazzetta ufficiale delle Comunità europee, C 48/8 del 13/3/1998 - che evidenzia l'attuale difficoltà a "controllare" in qualche forma l'uso del nuovo strumento.

Nella premessa il Consiglio ritiene che Internet sta diventando un'industria che offre servizi al grande pubblico con conseguenze positive soprattutto per l'istruzione, le fonti di informazione e così via. Si aggiunge subito dopo la riflessione sulle conseguenze negative che tale fenomeno ha già evidenziato: ci si preoccupa dei contenuti nocivi e illegali

diffusi da Internet ritenendolo un ostacolo per lo sviluppo e l'instaurarsi di un ambiente propizio alle iniziative.

Soprattutto per l'industria si avverte l'esigenza di un controllo dei contenuti o di strumenti di filtraggio per promuovere un ambiente sicuro.

Ricordiamo che la discussione dei problemi posti dal rapido sviluppo di Internet è sorta in ambito europeo fin dai primi mesi del 1996. Il Parlamento europeo nella sua risoluzione del 24 aprile 1997 ha invitato gli Stati membri a definire nei rispettivi ordinamenti giuridici norme minime comuni e forme di cooperazione, per raggiungere l'obiettivo comune di rendere sicuro l'uso di Internet.

La Dichiarazione ministeriale adottata alla Conferenza internazionale sul tema "Realizzare le potenzialità delle reti globali di informazione", tenutasi a Bonn il 6-8 luglio 1997, ha sottolineato il ruolo che il settore privato può assumere nella tutela degli interessi dei consumatori ed incoraggia l'industria ad escogitare sistemi di valutazione del contenuto e proporre servizi di valutazione adeguati alle esigenze dei vari utenti con la salvaguardia degli interessi della società in generale, compresi quelli dei produttori e dei consumatori. Senza addentrarci nella valutazione di merito sui sistemi di filtraggio o di controllo che introducono la discussione su argomenti come la limitazione della libertà o della forma di espressione, la riflessione sulla discussione comunitaria evidenzia la preoccupazione di tutti di voler prevenire le violazioni, soprattutto se commesse attraverso strumenti sconosciuti agli organi di controllo.

Sono ormai note le diverse storie degli *hackers*, conosciuti come "pirati informatici", non solo perché riescono a dimostrare di essere più bravi degli amministratori dei sistemi, ma perché riescono a procurare danni nelle più svariate forme.

L'impresa che decide di utilizzare i nuovi strumenti tecnologici non può sottovalutare il rischio che da essi ne potrebbe derivare.

Prendiamo il caso della diffusione dei *virus* o di programmi atti a danneggiare altri sistemi informatici attraverso il collegamento in Rete. In merito, uno studente della Cornell University, Robert Tappan Morris, fu condannato nel 1991 in America per aver infettato 6.000 *computer* con un *virus*, al fine di dimostrare che i sistemi adottati per impedire l'accesso non autorizzato a Internet erano assolutamente inaffidabili.

L'osservatorio sulla criminalità informatica - FTI - fin dal Rapporto del 1997, ha distinto due filoni di violazioni informatiche: gli atti commessi per mezzo di tecnologie informatiche e gli atti a danno dei sistemi informatici e telematici.

In entrambi i casi le difficoltà dell'accertamento sono legate all'uso dei sistemi tradizionali d'investigazione. A parte qualche gruppo isolato, in generale non esiste a livello nazionale un nucleo di Polizia giudiziaria che si occupa di tutte le violazioni informatiche. E potrebbe non bastare il solo nucleo specializzato per ogni provincia senza la collaborazione di esperti che vivono - per lavoro - nei diversi settori delle nuove tecnologie. Il punto debole della materia è che non basta più studiare a scuola o all'università l'informatica. La velocità dell'evoluzione tecnologica, ad esempio nel settore dell'*internetworking*, richiede un lavoro di gruppo per fronteggiare il fenomeno della pirateria, cioè di coloro che per passione o interessi vivono *full-time* nel mondo digitale.

I termini, piazze telematiche, realtà virtuali, città invisibili non sono più racconti tratti dai libri di fantascienza.

Tornando al fenomeno delle violazioni, esaminiamo il caso di un furto del numero di una carta di credito e proviamo ad esaminare il suo sviluppo. Colui che ha subito il furto potrà denunciare l'accaduto presso l'autorità giudiziaria. La denuncia sarà contro gli ignoti. La polizia giudiziaria delegata dal magistrato comincerà a prendere contatti con l'istituto di credito presso cui era stata rilasciata la carta di credito. A questo punto la Banca offrirà la massima collaborazione, ma non potrà far altro che indicare la provenienza della richiesta di addebito delle somme prelevate. Si scopre così che magari la richiesta è pervenuta dall'estero e che si è costretti a chiedere una rogatoria internazionale per proseguire le ricerche. A questo punto le difficoltà non sono più solo operative, ma cominciano i problemi tecnici. Chi preleverà i *log*, cioè il tracciato delle operazioni registrate? Come controllare la differenza del fuso orario con le mille difficoltà dei differenti sistemi operativi in uso, con la precaria affidabilità dei supporti contenenti i dati o con quant'altro di imprevedibile possa accadere ad un sistema telematico che è pur sempre soggetto ad avarie? In molti casi, se il furto è opera di esperti la ricerca non si limiterà ad un solo sistema. Si innesca il cosiddetto fenomeno del ping-pong o rimbalzo, cioè collegandosi a più sistemi prima di compiere la violazione.

Ci sono stati diversi episodi, per quanto riguarda i messaggi di posta elettronica, in cui attraverso i *remailer* anonimi, cioè dei *computer* che consentono di cambiare il proprio nome e addirittura di rendersi anonimi cancellando ogni traccia o identità del mittente, sono state compiute violazioni e danneggiamenti vari.

La soluzione del problema è da ricercarsi nell'equilibrio tra maggiore sicurezza e migliori tecniche di accertamento delle violazioni. È vero che entrare in un'abitazione con la porta aperta o senza una parete è pur sempre violazione di domicilio e della proprietà privata, ma a quel punto bisogna punire anche la semplice curiosità.

Per finire, non sono le nuove norme che occorrono! Qualcuno già due secoli fa disse che le troppe leggi, che il cittadino non poteva conoscere a memoria, erano peggio delle poche leggi! Bisogna trovare il metodo per seguire, a vista d'occhio, l'evoluzione dell'informatica e della telematica, con gli strumenti a disposizione in quel momento.

8. NOTA BIBLIOGRAFICA

CILLI A., *Questioni di contratti* - Internet news, Tecniche nuove, aprile 1998.

FTI *Rapporto 1998*, Franco Angeli, 1998.

HANCE O., *Internet e la legge*, McGraw-Hill, 1997.

LARRY J., HUGES JR., *Tecniche di sicurezza Internet*, Jackson libri, 1996.

TORRENI O., PARIRE S., *Internet e diritto* - Il Sole 24 Ore, Norme e Tributi, 1997.

9. APPENDICE

Diapositiva 1

La sicurezza delle transazioni nel commercio elettronico

ALCUNE CIFRE

Transazioni on-line a livello mondiale:

- nel 1998 --> spese oltre 48 miliardi di dollari
- nel 2002 --> supereranno i 410 miliardi di dollari
- nel 2005 --> raggiungeranno i 3.000 miliardi

SITUAZIONE ITALIANA

- il 1998 è stato il primo anno significativo per il commercio elettronico
- per il 1999 è prevista la spesa di 800 miliardi
- per i primi anni del nuovo millennio la crescita è esponenziale

Copyright © 99 by Antonio Cilli



Diapositiva 2

La sicurezza delle transazioni nel commercio elettronico

DILEMMA: VANTAGGI/RISCHI

VANTAGGI:

- velocità
- attrattiva
- accessibilità 24 ore su 24
- apertura 7 giorni su 7

RISCHI:

- clienti e venditori non si possono guardare
- non è possibile controllare firme e carte d'identità
- è facile copiare la grafica del negozio virtuale

Copyright © 99 by Antonio Cilli



Diapositiva 3

La sicurezza delle transazioni nel commercio elettronico

DILEMMA: VANTAGGI/RISCHI**RISCHI:**

- alcuni negozi hanno preso illegalmente i numeri di carta di credito
- numerose transazioni sono state intercettate
- sono stati sviluppati software in grado di generare numeri di carte di credito
- sono stati creati canali di chat per lo scambio di notizie sulle truffe con il pagamento on-line
- in molti casi non è stato implementato alcun sistema di sicurezza per il pagamento on-line

Copyright © 99 by Antonio Cilli

Diapositiva 4

La sicurezza delle transazioni nel commercio elettronico

TRANSAZIONI ON-LINE**COS'E' IL PAGAMENTO ON-LINE?**

- il cliente acquista e paga con Carta di credito
- il negoziante chiede alla Banca del cliente la disponibilità e l'accredito
- la merce viene spedita

**I SISTEMI DI PAGAMENTO
GIOCANO IL RUOLO PIU' IMPORTANTE!
E' frequente leggere la seguente avvertenza:
"SI SCONSIGLIA L'USO DELLA CARTA DI
CREDITO IN CHIARO"**

Copyright © 99 by Antonio Cilli

Diapositiva 5

La sicurezza delle transazioni nel commercio elettronico

I SISTEMI DI PAGAMENTO

- * La prima forma fu il BARATTO
- * Nel 15° secolo nacquero le BANCHE
- * Nella 2° metà del '900 è avvenuta la rivoluzione:
attraverso l'informatica e la telematica



DISTINZIONE DEI SISTEMI DI PAGAMENTO:

- **SISTEMI BASATI SU SOLUZIONI HARDWARE**
- **SISTEMI BASATI SU SOLUZIONI SOFTWARE**

Copyright © 99 by Antonio Cilli

Diapositiva 6

La sicurezza delle transazioni nel commercio elettronico

SISTEMI BASATI SU SOLUZIONI HARDWARE
(Pagamento attraverso carte prepagate)



VANTAGGI:

- facilità di diffusione delle carte attraverso:
 - biglietterie
 - distributori automatici
 - giornali

SVANTAGGI:

- creazione di uno standard di carte
- implementazioni di lettori sui PC
- livelli di sicurezza accettabili

Copyright © 99 by Antonio Cilli

Diapositiva 7*La sicurezza delle transazioni nel commercio elettronico***SISTEMI BASATI SU SOLUZIONI SOFTWARE**
(numerosa proposte)**DISTINZIONE IN 3 CLASSI:**

1. Utilizzo di carte di credito
2. Impiego di assegni digitali
3. Utilizzo della moneta elettronica

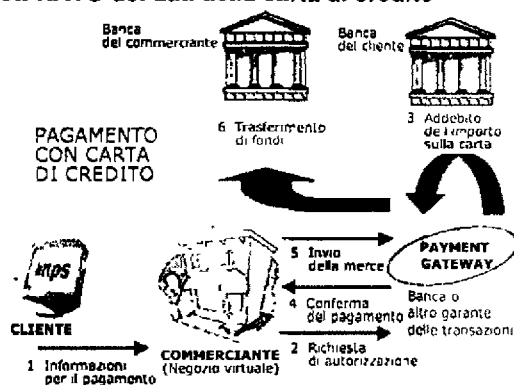
PAGAMENTO CON CARTA DI CREDITO

- ordine del prodotto e comunicazione del numero di carta per fax o per telefono
- acquisto ed invio in CHIARO dei dati della carta di credito (**RISCHIO DI INTERCETTAZIONE**)

Copyright © 99 by Antonio Cilli

Diapositiva 8*La sicurezza delle transazioni nel commercio elettronico***PAGAMENTO CON CARTA DI CREDITO**

- invio **CIFRATO** dei dati della carta di credito



Diapositiva 9

La sicurezza delle transazioni nel commercio elettronico

ASSEGNI DIGITALI

Presupposto:

Attivazione di un conto presso una BANCA ON-LINE



Utilizzo/Vantaggi:

- Compilazione di un assegno digitale
- Utilizzo di protocolli come SSL o SET per la codifica dei dati
- Richiesta di pagamento attraverso la propria banca di fiducia
- Rapidità del pagamento

Informazioni su alcuni sistemi sperimentati:

<http://gost.isi.edu/info/netcheque/distribution.htm>

Copyright © 99 by Antonio Cilli

Diapositiva 10

La sicurezza delle transazioni nel commercio elettronico

MONETA ELETTRONICA

COM'E' IL DENARO O UNA BANCONOTA VIRTUALE

E' costituita da una lunga serie di bit generata da un software



COME FUNZIONA

- L'acquirente fabbrica la banconota e la manda alla propria banca
- La banca verifica la disponibilità e rispedisce la banconota apponendovi un numero di serie

ASPETTO SICUREZZA?

NECESSARI ALGORITMI DI CRITTOGRAFIA

Copyright © 99 by Antonio Cilli

Diapositiva 11

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA

Protocollo SSL (Secure Socket Layer) come funziona

- CRIPTA le informazioni dal browser al sito Web
- Rende illegibili le informazioni intercettate



Come si riconosce chi lo usa?

Il protocollo S-Http (Secure Hypertext Transfer Protocol) instaura il collegamento sicuro:

- appare un lucchetto o una chiave
- il protocollo cambia da HTTP a HTTPS



COSA MANCA?

La certezza sull'identità di chi effettua la transazione!

Copyright © 99 by Antonio Cilli

Diapositiva 12

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA

NELL'USO DEL PROTOCOLLO DI SICUREZZA:

- Manca la firma, l'identità di chi effettua l'operazione
- E' ripudiabile dal legittimo titolare



VANTAGGI

- E' un sistema semplice e veloce
- Ha avuto molto successo:
es. amazon.com ---> oltre 9 milioni di clienti

NUOVI PROTOCOLLI: SET (Secure Electronic Transfer)

Copyright © 99 by Antonio Cilli

Diapositiva 13

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA**IL PROTOCOLLO SET (Secure Electronic Transfer)**

Non è integrato in tutti i browser

E' necessario l'installazione di un software

Il titolare deve chiedere il rilascio di un codice personale (PIN)

Le transazioni non sono ripudiabili da parte del titolare

L'onere della prova è a carico del titolare

CERTIFICATI DIGITALI:

E' un documento elettronico reso valido da una

CERTIFICATION AUTHORITY

es. VERISIGN --> (www.verisign.com)

Copyright © 99 by Antonio Cilli

**Diapositiva 14**

La sicurezza delle transazioni nel commercio elettronico

SITUAZIONE ITALIANA

• SONO STATI SPERIMENTATI E RESI DISPONIBILI MOLTI SISTEMI

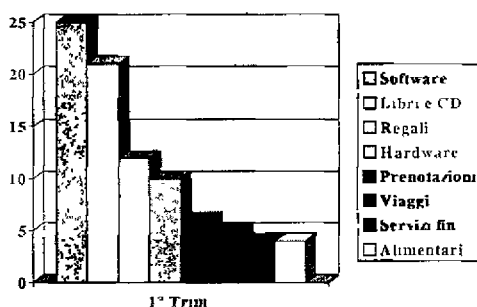
• ESISTE LA POSSIBILITA' DI FORMARE ED INVIARE UN DOCUMENTO INFORMATICO ASSICURANDO LA SUA INTEGRITA'

• ESISTONO SOFTWARE DI CRITTOGRAFIA A CHIAVE PUBBLICA

es. PGP (Pretty Good Privacy) di Zimmerman utilizza 2 algoritmi di crittografia: a chiavi pubbliche RSA e a chiavi private IDEA

Copyright © 99 by Antonio Cilli



*Diapositiva 15**La sicurezza delle transazioni nel commercio elettronico***ACQUISTI IN RETE IN ITALIA NEL 1998***Copyright © 99 by Antonio Cilli**Diapositiva 16**La sicurezza delle transazioni nel commercio elettronico***PRECAUZIONI PER L'USO****"SCONSIGLIAMO L'UTILIZZO IN CHIARO DEL VOSTRO****NUMERO DI CARTA SU INTERNET"**
oppure**"I SISTEMI DI SICUREZZA ATTUALMENTE IN USO NON
SONO PIENAMENTE RICONOSCIUTI DAI CIRCUITI
INTERNAZIONALI VISA E MASTERCARD/EUOCARD"****Consultabile al seguente indirizzo Internet:
<http://www.cartasi.it/java/istruzioni.html>***Copyright © 99 by Antonio Cilli*

Diapositiva 17

La sicurezza delle transazioni nel commercio elettronico

Siti di riferimento:



<http://www.netgallery.net/ecommerce>

<http://www.cybercash.com>

<http://www.digicash.com>

<http://www.netmarket.com>

<http://www.visa.com>

<http://www.cert.org>

<http://web.mit.edu>

<http://www.aipa.it>

<http://www.rsa.com>

<http://www.pgpi.com>

Copyright © 99 by Antonio Cilli