

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Smart card, trasmissioni televisive cifrate e reati informatici

Gianluca Pomante¹

Il commento di una sentenza dovrebbe essere sereno e pacato, e limitarsi ad evidenziare gli elementi positivi e negativi riportati in fatto e in diritto, soprattutto quelli che hanno determinato l'orientamento del giudice, permeando la motivazione del provvedimento.

Eppure, nell'esaminare la sentenza della Suprema Corte di Cassazione - Sez. V penale, n. 1904 del 27 marzo 1998, nonché l'Ordinanza del Tribunale Penale di Genova - Sez. II penale, del 27 gennaio 2000, di pari oggetto, è ben difficile commentare con oggettività e distacco la manifesta ignoranza (*rectius: colui che ignora*) che i giudici mostrano nell'approccio alla materia.

Il riesame di provvedimenti cautelari di natura reale non è particolarmente interessante per un magistrato, e costituisce probabilmente una noiosa routines alla quale non può sottrarsi. Tuttavia, non si può che sorridere (per non piangere) dinanzi a motivazioni che evidenziano come - in base al ragionamento estrinsecato nei distinti provvedimenti - dovremmo allora considerare sistemi informatici anche la lavatrice e la lavastoviglie, solo perché programmabili e in grado di gestire i dati provenienti da numerosi sensori.

Chissà che quanto prima non venga contestata la fattispecie di reato di cui all'art. 615-ter c.p. ad un soggetto 'reo' di essersi 'abusivamente introdotto' nella lavatrice della propria consorte, allo scopo di stendere i panni, violandone così la 'misura di sicurezza' consistente nella serratura apposta all'oblò.

Scherzi a parte, nei casi in esame si discute dell'ammissibilità o meno della misura cautelare in presenza di *smart card*, di chiavi per la decrittazione di trasmissioni cifrate, di apparati idonei a leggere e programmare dette carte a microprocessore.

Che l'inciviltà tecnologica abbia ormai raggiunto il proprio apice è un dato di fatto, ed è altrettanto evidente che la disponibilità di strumenti informatici di notevole potenza a basso costo ha reso più facile la violazione di diritti personali e patrimoniali rispetto al passato.

Ma ciò non significa che ogni comportamento apparentemente non in linea con l'ordinamento sia necessariamente di rilevanza penale. Il giudice, nell'esercizio delle sue funzioni, dovendo mantenersi imparziale e distaccato ed assumere il ruolo di soggetto *super partes* che gli è naturale, ha l'obbligo di informarsi e documentarsi adeguatamente prima di assumere decisioni che avranno pesanti riflessi sulle condizioni personali e patrimoniali di un soggetto.

¹ In Internet all'indirizzo www.pomante.com

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Ciò non è avvenuto nei casi che qui si commentano e che appaiono invece giudicati frettolosamente e 'secondo la moda'; ne sono la riprova i provvedimenti scaturiti dai giudizi di riesame, che evidenziano come i magistrati abbiano pedissequamente accolto la tesi della Polizia Giudiziaria, omettendo di assumere informazioni banali e note perfino ai ragazzini che giocano con la Playstation.

Nel caso pervenuto all'esame della Suprema Corte il ricorrente contestava la legittimità del provvedimento di sequestro asserendo che la commercializzazione a mezzo Internet di schede e codici per la decrittazione di segnali televisivi non poteva essere ricondotta alla fattispecie di reato di cui all'art. 615-*quater*.

Sia il Tribunale di Torino che la Corte di Cassazione propendevano per il rigetto dell'istanza sostenendo che ben poteva ritenersi «la televisione in abbonamento, alla quale può accedersi soltanto tramite un decoder a pagamento in grado di decrittare il segnale televisivo ... un sistema informatico o telematico protetto da misure di sicurezza».

Già la circostanza che i magistrati della Suprema Corte utilizzino i termini 'sistema informatico' e 'sistema telematico' come sinonimi evidenzia l'assoluta inidoneità del collegio giudicante ad assumere provvedimenti in materia.

In un analogo macroscopico errore incorreva il Tribunale del riesame di Genova con l'ordinanza del 27 gennaio 2000, allorchè il collegio asseriva «non pare potersi negare al sistema di trasmissione – ricezione di tali comunicazioni (segnale satellitare criptato) la qualifica di sistema telematico». In questo caso sono i termini 'sistema di trasmissione' e 'sistema telematico' ad essere erroneamente usati come sinonimi.

Appare evidente come i magistrati investiti della vicenda confondano i sistemi informatici con i sistemi elettronici. Ogni sistema informatico è un sistema elettronico, giacchè l'elettronica è alla base dei componenti che fanno parte di esso. Ma non è sempre vero il contrario.

Un forno a microonde è un sistema elettronico, ma non è un sistema informatico, analogamente ad una lavatrice, ad un impianto hi-fi, ad un videoregistratore, ecc.

Il sistema informatico, il sistema telematico ed il sistema di trasmissione sono indubbiamente sistemi elettronici ma ciò non basta per affermare che siano identici e sostituibili e che i termini che li individuano possano essere usati come sinonimi.

Per comprendere quale sostanziale differenza sussista tra un sistema informatico, un sistema telematico e un sistema di trasmissione (via cavo, via etere o satellitare poco importa), sarebbe stato sufficiente consultare una comune enciclopedia.

Il *sistema informatico* è l'insieme dei componenti *hardware* e *software* che consentono il trattamento automatico dei dati, ossia l'apparecchiatura che viene comunemente chiamata elaboratore o computer unitamente ai programmi e dati che le permettono di funzionare.

Due o più sistemi informatici, collegati tra loro per mezzo di reti di telecomunicazione, danno vita ad un *sistema telematico*, la cui caratteristica

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

fondamentale è quella di poter scambiare dati. Ne è attualmente il miglior esempio la rete Internet.

La caratteristica essenziale di un *sistema di trasmissione*, invece, è proprio quella di non poter scambiare i dati, ma di inviarli (stazione trasmittente) ad un numero indeterminato di apparati in grado di riceverli (stazioni riceventi), come avviene per le trasmissioni televisive, sia tradizionali che criptate. Ne sono un esempio proprio i sistemi – basati su tecnologia satellitare - utilizzati dalle aziende coinvolte, come parti offese, nei procedimenti penali di cui si commentano i provvedimenti di riesame.

La circostanza che molti apparati radiotelevisivi siano gestiti mediante sistemi informatici è solo la conseguenza dell'attuale stato dell'arte della tecnologia di settore. Ma non era tale la situazione in passato e, probabilmente, non lo sarà in futuro se la tecnologia informatica seguirà strade diverse rispetto a quella propria dei sistemi di trasmissione.

Il semplice utilizzo di un elaboratore per miscelare i segnali audio e video o per controllare un antenna o un ripetitore non è sufficiente a qualificare l'intero sistema come 'telematico'.

Si tratta di sistemi distinti, seppure utilizzabili sinergicamente, aventi ciascuno proprie caratteristiche e proprie peculiarità.

Sono, questi, elementi noti anche ai bambini che giocano con le biglie; sembrano invece sconosciuti ai magistrati.

È sufficiente osservare (senza che sia necessario neppure capire come ciò avvenga) una comunicazione tramite Netmeeting (o altro software di *videoconferencing*) ed una comunicazione tramite radio ricetrasmittenti.

Chi utilizza quest'ultime deve attendere il proprio turno per parlare e, ad ogni sessione, deve annunciare la fine del proprio discorso con il famoso 'passo', cosa che non avviene con il Netmeeting e programmi analoghi.

Il sistema di trasmissione (satellitare, via cavo o via radio, poco importa) funziona in una sola direzione e tanto ciò è vero che le aziende che erogano tale servizio non possono conoscere il numero e la posizione dei decoder in funzione. Se il sistema di trasmissione fosse anche solo simile ad un sistema telematico, sarebbe possibile accertare in ogni momento quanti e quali decoder sono in funzione, verificare la conformità del funzionamento di ciascuno con il tipo di abbonamento sottoscritto, denunciare ogni abuso e così via. Proprio come avviene per Internet, mezzo telematico per eccellenza, collegandosi al quale si viene indissolubilmente legati, per l'intera sessione di lavoro, ad un indirizzo elettronico (IP address) che consente di tracciare e monitorare ogni comportamento dell'utente.

Cosa pensano i sedicenti esperti della materia? Che le aziende si lascerebbero sfuggire una simile occasione di controllare, monitorare e schedare gli utenti? O di reprimere abusi commessi ai loro danni?

La TV interattiva non è ancora una realtà e ciò dipende proprio da questa caratteristica dei sistemi di trasmissione. Ne è la riprova il servizio *'pay per view'*

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

attivato, ad esempio, da Stream e Tele+, per fruire del quale è necessario collegare il decoder alla linea telefonica, affinché l'azienda possa conoscere le richieste dell'utente ed inviare al decoder un segnale di attivazione della smart card che consenta di visionare il programma scelto.

Proprio tale operazione da compiere dimostra che il decoder non è in grado di scambiare dati con la stazione che trasmette i programmi; diversamente la linea telefonica sarebbe inutile.

Solo con l'integrazione tra sistemi telematici e sistemi di trasmissione sarà possibile raggiungere l'obiettivo della TV interattiva. Ed infatti sono allo studio diversi progetti per integrare Internet con la televisione ed attivare così in modo permanente quel 'canale di ritorno' che ora manca ai sistemi di trasmissione e che impedisce il dialogo con gli utenti.

Allo stato attuale ciò non è possibile, perché ogni sistema di trasmissione basa il suo funzionamento sull'invio di un segnale che viene poi captato dai sistemi di ricezione indipendentemente dalla fonte.

Segnale che, per tali motivi, non viene diretto su determinati punti, ma irradiato sull'intero territorio coperto dalla potenza dell'impianto.

Non è questa la sede per approfondire ulteriormente l'elemento tecnico, ma è evidente il macroscopico e grossolano errore commesso dai magistrati che hanno assunto i provvedimenti in esame.

Semmai l'utilizzo di *smart card* modificate per l'intercettazione abusiva di trasmissioni televisive (perché questo è il comportamento concreto da tenere in considerazione) potrebbe rientrare nelle fattispecie di cui agli artt. 617 quater e quinquies c.p. (*Intercettazione di comunicazioni informatiche o telematiche e Installazione di apparecchiature atte ad intercettare comunicazioni informatiche o telematiche*) che, per effetto del disposto normativo di cui all'art. 623 c.p. (*Altre comunicazioni e conversazioni*) vengono estese fino a ricomprendere ogni altro comportamento delittuoso inerente la trasmissione a distanza di suoni, immagini o altri dati, senza che possa farsi alcuna distinzione circa il tipo di sistema utilizzato a tal fine.

Strano che i giudici di merito e di legittimità, così attenti nel ricercare un'ardita interpretazione degli artt. 615-ter e quater, non abbiano letto il codice penale fino alla Sezione V del titolo XIII, che è invece certamente più adatta al comportamento contestato agli indagati.

Del resto, anche la collocazione sistematica della norma (*Inviolabilità dei segreti*) appare più consona a quella dei reati ipotizzati dai magistrati di Genova e Torino (*Tutela del domicilio*).

La tutela dell'inviolabilità dei segreti può essere stiracchiata fino a ricomprendere e proteggere qualsiasi comunicazione; sostenere la violazione dell'altrui domicilio per aver captato e decodificato un segnale diffuso nell'etere sembra decisamente inadeguato (senza peraltro voler entrare nel merito dell'affidabilità dell'algoritmo di

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

cifratura e della responsabilità di quanti lo hanno utilizzato per proteggere le trasmissioni).

Salvo che qualcuno non voglia sostenere che, attraverso la modifica delle smart card, si possa utilizzare il decoder per introdursi abusivamente nelle stazioni radiotelevisive o nei satelliti per telecomunicazioni; ma in tal caso, a parte i problemi di giurisdizione legati alla violazione di un presunto 'domicilio satellitare', sarebbe forse più opportuno non dilettersi in disquisizioni dottrinali ma procedere ad allertare il servizio psichiatrico delle ASL competenti per territorio.

Battute a parte, neppure le fattispecie di cui al combinato disposto degli artt. 617 quater, 617-*quinquies* e 623 c.p. sarebbero concretamente applicabili ai casi in esame, per un motivo talmente evidente e banale da essere sfuggito a tutti i magistrati che si sono occupati della vicenda: le *smart card* del tipo utilizzato per la decodifica di trasmissioni televisive non sono reperibili in commercio e non possono essere acquisite (vengono concesse in comodato) senza sottoscrivere un abbonamento ai servizi erogati dalle aziende che trasmettono i programmi criptati.

Ebbene, se è stato stipulato un contratto di abbonamento appare di tutta evidenza che manca il presupposto giuridico per procedere penalmente, dato che l'abuso si concretizza in una mera violazione contrattuale consistente nell'accedere ad un servizio più esteso di quello per il quale si è pagato il corrispettivo.

In capo alle aziende interessate, pertanto, sussiste il mero diritto di richiedere la differenza tra il prezzo pagato e il servizio di cui ha effettivamente fruito l'utente. Se un individuo sottoscrive un qualsiasi abbonamento, nel momento in cui valica i limiti previsti dal contratto viene invitato a pagare la differenza di prezzo dovuta per il maggior servizio erogato dall'azienda in suo favore. Certamente non sarà possibile richiedere l'intervento delle Forze dell'Ordine e denunciare il cliente per furto o per frode. Per quale motivo, pertanto, dovrebbe procedersi diversamente nel caso dei servizi fruibili tramite smart card?

È forse troppo banale tale soluzione? Oppure è semplicemente più economico, per le aziende, richiedere l'intervento delle Forze dell'Ordine e della Magistratura - pagati con il denaro pubblico - rispetto al dover azionare innumerevoli, singoli giudizi civili - di cui dovrebbero sostenere le spese - contro gli utenti colpevoli di aver fruito di servizi in misura maggiore del corrispettivo pagato?

Di certo l'effetto prodotto dal semplice avvio di un procedimento penale, nell'opinione pubblica, anche grazie alla risonanza data dai mass-media agli avvenimenti, è notevole e ben più efficace di migliaia di sentenze civili, pur favorevoli.

Infine, a conferma della superficialità con cui vengono trattati i procedimenti di riesame, non appare inutile sottolineare quanto contenuto nell'ordinanza del Tribunale di Genova, ove si legge, testualmente: «Preliminarmente devono svolgersi alcune spiegazioni in ordine al materiale sequestrato, la cui natura emerge dai documenti integrativi trasmessi dal P.M.. Appare opportuno segnalare che in questa

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è SMART CARD, TRASMISSIONI TELEVISIVE CIFRATE E REATI INFORMATICI, GIANLUCA POMANTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO III, PP. 371-379. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

fase processuale, non potendosi ricorrere a perizia, il collegio non può che affidarsi ai dati emergenti dagli atti processuali, anche in ordine alla spiegazione tecnica sugli oggetti del sequestro e sul loro funzionamento. In particolare dunque risulta dalla relazione della p.g...».

Interessante argomentazione. Se ogni procedimento di riesame – durante il quale, almeno secondo quanto viene ancora insegnato nelle Università, il Collegio dovrebbe valutare il corretto operato del Pubblico Ministero e della Polizia Giudiziaria - dovesse essere basato sui chiarimenti e sugli atti trasmessi all'organo giudicante proprio dal Pubblico Ministero e dalla Polizia Giudiziaria, tanto varrebbe abrogare questa parte del Codice di Procedura Penale.

Ogni ulteriore commento appare superfluo.