

**Indagine informatica e garanzie:  
l'individuazione del responsabile,  
il tempus ed il locus commissi delicti**

**Cesare Parodi-Procura della Repubblica  
di Torino**

# **CRITICITA'**

**denuncia a carico di ignoti**

**dove è avvenuta la condotta ?**

**dove è avvenuto l'evento ?**

**quando è avvenuta la condotta?**

**aumento esponenziale delle  
denunce/querele**

**assoluta delocalizzazione del  
conseguimento del profitto**

**assoluta necessità di coordinamento  
nazionale e internazionale**

**necessità di “ fare i conti” con lo strumento  
dell’assistenza giudiziaria internazionale**

## I LIMITI SOSTANZIALI: L'ART. 6 C.P.

### **Reati commessi nel territorio dello Stato.**

Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana.

Il reato si considera commesso nel territorio dello Stato , **quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione.**

## Art. 10.

### Delitto comune dello straniero all'estero.

Lo straniero, che ..... commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce la pena di morte o l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del ministro della giustizia, ovvero istanza o querela della persona offesa.

## IL FATTORE TEMPO

D.lgs 196/2003 modificato dal d.lgs. 109/2008

Art. 132 (Conservazione di dati di traffico per altre finalità).

.... i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i **dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.**

**I DATI SONO RICHIESTI DAL PM DIRETTAMENTE**

## Riforma Alfano sulle Intercettazioni **Art. 266. c.p.p.**

L'intercettazione di conversazioni o comunicazioni telefoniche, di altre forme di telecomunicazione, di immagini mediante riprese visive e **l'acquisizione della documentazione del traffico delle conversazioni o comunicazioni** sono consentite nei procedimenti relativi ai seguenti reati:.....

## Art. 267 c.p.p.

Il pubblico ministero, **con l'assenso scritto del procuratore della Repubblica, ovvero del procuratore aggiunto o del magistrato appositamente delegati**, richiede l'autorizzazione a disporre le operazioni previste dall'articolo 266 al **tribunale del capoluogo del distretto** nel cui ambito ha sede il giudice competente, che decide in **composizione collegiale**.

L'autorizzazione è data con decreto, motivato contestualmente e non successivamente modificabile o sostituibile, quando vi sono evidenti **indizi di colpevolezza** e le operazioni previste dall'articolo 266 sono assolutamente indispensabili ai fini della prosecuzione delle indagini e **sussistono specifiche e inderogabili esigenze** relative ai fatti per i quali si procede, fondate su elementi **espressamente e analiticamente indicati nel provvedimento**, non limitati ai soli contenuti di conversazioni telefoniche intercettate nel medesimo procedimento e frutto di un'autonoma valutazione da parte del giudice.

!!!!!!



## **Art. 266 bis c.p.p.**

Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è **consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.**

**NON RISULTA MODIFICATO**

**E i reati non ricompresi nel nuovo art. 266 ???**

**COSA ACCADE PER LA DOCUMENTAZIONE DEL  
TRAFFICO ?**

**a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della  
reclusione superiore nel massimo a cinque anni determinata a norma  
dell'articolo 4;**

.....

**f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di  
informazioni privilegiate, manipolazione del mercato, molestia o  
disturbo delle persone col mezzo del telefono;**

**g) delitti previsti dall'articolo 600-ter, terzo comma, del codice penale,  
anche se relativi al materiale pornografico di cui all'articolo 600-  
quater.1, del medesimo codice.**

AD ESEMPIO:

Art. 615 ter c.p. accesso abusivo

615 quater c.p. detenzione codici di accesso

635 bis c.p. danneggiamento

640 ter c.p. frode informatica

# ISCRIZIONI e GARANZIE

ART. 335 C.P.P.

*Sez. U, Sentenza n. 16 del 21/06/2000 Ud. (dep. 30/06/2000 )*  
*Rv. 216248*

L'omessa annotazione della "notitia criminis" nel registro previsto dall'art. 335 c.p.p., con l'indicazione del nome della persona raggiunta da indizi di colpevolezza e sottoposta ad indagini "contestualmente ovvero dal momento in cui esso risulta", **non determina l'inutilizzabilità degli atti di indagine compiuti sino al momento dell'effettiva iscrizione nel registro**, poiché, in tal caso, il termine di durata massima delle indagini preliminari, previsto dall'art. 407 c.p.p., al cui scadere consegue l'inutilizzabilità degli atti di indagine successivi, decorre per l'indagato **dalla data in cui il nome è effettivamente iscritto nel registro delle notizie di reato**, e non dalla presunta data nella quale il pubblico ministero avrebbe dovuto iscriverla.

*Sez. U, Sentenza n. 16 del 21/06/2000 Ud. (dep. 30/06/2000 ) Rv. 216248*

L'apprezzamento della tempestività dell'iscrizione, **il cui obbligo nasce solo ove a carico di una persona emerga l'esistenza di specifici elementi indizianti e non di meri sospetti**, rientra nell'esclusiva valutazione discrezionale del pubblico ministero ed è sottratto, in ordine all'"**an**" e al "**quando**", al sindacato del giudice, ferma restando la configurabilità di ipotesi di responsabilità disciplinari o addirittura penali nei confronti del p.m. negligente.

*Sez. 5, n. 1410 del 21/09/2006 Cc. (dep. 19/01/2007 ) Rv. 236029*

La tardiva iscrizione del nome dell'indagato nel registro di cui all'art. 335 c. p. p. non determina alcuna invalidità delle indagini preliminari ma consente, tuttavia, **al giudice di rideterminarne il termine iniziale**, in riferimento al momento in cui si sarebbe dovuta iscrivere la notizia di reato; ne deriva che la **tardiva iscrizione può incidere sulla utilizzabilità delle indagini finali ma non sulla utilizzabilità di quelle svolte prima della iscrizione** e che il relativo accertamento non è censurabile in sede di legittimità qualora sia sorretto da congrua e logica motivazione.

## Le prospettive di riforma

- all'articolo 405 sono apportate le seguenti modificazioni:

...

2) il comma 2 è sostituito dal seguente:

«2. Salvo quanto previsto dall'articolo 415-bis, il pubblico ministero richiede il rinvio a giudizio entro sei mesi dalla data in cui il nome della persona alla quale è attribuito il reato è iscritto nel registro delle notizie di reato ovvero dalla data in cui risulta il nome della persona alla quale il reato è attribuito, ai sensi dell'articolo 335, comma 1. A tal fine il giudice verifica l'iscrizione operata dal pubblico ministero e determina la data nella quale essa doveva essere effettuata, anche agli effetti dell'articolo 407, comma 3»;



## 407 comma 3 c.p.p.

3. Salvo quanto previsto dall'articolo 415-bis, qualora il pubblico ministero non abbia esercitato l'azione penale o richiesto l'archiviazione nel termine stabilito dalla legge o prorogato dal giudice, gli atti di indagine compiuti dopo la scadenza del termine non possono essere utilizzati.

c) all'articolo 407, dopo il comma 3 è aggiunto il seguente:

«3-bis. Quando il pubblico ministero trasmette per competenza gli atti ad altra autorità giudiziaria, nonché in ogni altro caso in cui si verifica la regressione del procedimento alla fase delle indagini preliminari, se i termini di cui ai commi 1 e 2 sono scaduti, le indagini possono essere proseguite **per un periodo non superiore a sei mesi**»

## E allora: quando si deve iscrivere il “nome”?

Non c'è una foto, un filmato o una identificazione formale: prova logica e presuntiva.

Specifici elementi indizianti e non solo meri sospetti

Due passaggi obbligati: reperire l'account e l'utenze e quindi reperire l'autore “fisico” della condotta. Che potrebbe non coincidere con il beneficiario della stessa....

**L'indagine tradizionale:  
accertamento giorno ed ora del fatto ed acquisizione file di log  
e quindi dal file di log all'utenza telefonica  
d.lgs. 109/2008**

**Categorie di dati da conservare per gli operatori di telefonia e  
di comunicazione elettronica**

**Obblighi dei gestori di Internet Point**

**L'“indifferenza” del Provider all'accertamento dell'identità dell'utente  
non può che essere strettamente dipendente dalla misura in cui il sistema  
giuridico nell'insieme chiamerà il Provider stesso a rispondere, in  
termini civili o penali, dei comportamenti posti in essere dall'utente  
tramite il proprio server.**

*Sez. 5, n. [6046](#) del 11/11/2008 Ud. (dep. 11/02/2009 ) Rv. 242960*

**Non sussiste la responsabilità del gestore di un punto internet a titolo di diffamazione per non avere impedito l'evento (art. 40, comma secondo, e 595 cod. pen.) qualora l'utente invii una e-mail avente contenuto diffamatorio, in quanto il gestore non solo non ha alcun potere di controllo e, quindi, alcuna conoscenza sul contenuto della posta elettronica inviata, ma gli è addirittura **impedito di prenderne contezza** - ex art. 617 quater c.p. che vieta l'intercettazione fraudolenta di sistemi informatici e telematici - mentre ha **l'obbligo di identificare gli utenti** che facciano uso del terminale ai soli fini della prova dell'utilizzazione e non per impedire l'eventuale reato.**

# Un fatto illecito può provenire:

- **da un singolo computer**, collegato tramite modem alla rete ( in tale situazione l'individuazione dell'autore del reato non presenta particolari difficoltà, o quantomeno non si pone in termini problematici significativamente differenti da quelli relativi ai reati "comuni")
- **dall'interno di un sistema**, da parte di un operatore di quest'ultimo che intervenga su una specifica stazione di lavoro del sistema medesimo (non necessariamente tuttavia l'operatore di "quella" stazione di lavoro)
- **da un intero "sistema"** ( Intranet) senza possibilità di individuare la specifica stazione di lavoro da una delle sopra indicate provenienza, ma abusivamente ad opera di un soggetto terzo che abbia posto in essere un "ponte" per porre in essere un reato approfittando di una connessione autorizzata: l'utente può utilizzare in modo fraudolento l'identificativo di un altro utente ovvero alterare il proprio indirizzo elettronico.

# LA PROVENIENZA “PRIVATA”

- **E' sufficiente per l'iscrizione la titolarità dell'utenza o dell'account?**
  
- **Generalmente NO: occorre una verifica ulteriore:**
  - **stato di famiglia/situazione di convivenza**
  - **perquisizioni e verifiche su concreto utilizzo p.c. e/o utenze**
  - **verifica – ove possibile- del “movente”.**

# **LA PROVENIENZA da “ENTE/PERSONA GIURIDICA”**

**Per motivi- anche – di sicurezza- tali soggetti dovrebbero assicurare la “tracciabilità” della attività interne: ad ogni connessione dovrebbe corrispondere un nominativo.**

**E se non avviene? C'è sicuramente colpa, ma come si prova il dolo e quindi l'eventuale concorso ?**

**E quindi: chi si iscrive ???**

**Vedi punto precedente, per ricerca elementi oggettivi e/o movente....**

**Utilizzo di account “sottratti”, con sostituzione ad altro soggetto (che non aveva creato l’account”) o con “usurpazione di account esistente.**

*Sez. 5, n. [46674](#) , 8/11/2007 Ud. (dep. 14/12/2007 ) Rv. 238504*

**Integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale).**



# ULTERIORI DIFFICOLTA'

- reti wireless
- anonymous remailer
- cancellazione dei file di log
- creazione di account con nomi di fantasia
- controllo di p.c. altrui....

# WI-FI....

**E se il numero Ip corrisponde a una persona che ha  
una wi-fi unlocked?**

**Chiunque può connettersi....**

**E' necessaria l'iscrizione ?**

**Se possibile, occorre una verifica di elementi ulteriori,  
informatici e non**

# **IL “FENOMENO” E-BAY**

**Non viene inviato l’oggetto pagato**

**Se non sussistono specifici elementi di sospetto:  
inadempimento civilistico.**

**Obbligo di iscrizione del beneficiario dell’accredito per il solo fatto della  
ricezione del pagamento ?**

**E il beneficiario di un pagamento effettuato con carta di credito  
indebitamente utilizzata ?**

**Ipotesi: sarebbe accolta una richiesta di assistenza internazionale  
sulla base di tale solo elemento?**

# LE REGOLE SULLA COMPETENZA

## I REATI “PATRIMONIALI”- l’art. 640 ter

- *Sez. 6, n. [3065](#) del 04/10/1999 Cc. (dep. 14/12/1999 ) Rv. 214942*

Il reato di frode informatica (art. 640 ter cod. pen.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui.

- *Sez. 5, n. [2672](#) del 19/12/2003 Cc. (dep. 27/01/2004 ) Rv. 227816*

- Il delitto di **accesso abusivo** a un sistema informatico previsto dall'art. 615-ter cod. pen. può concorrere con quello di **frode informatica** di cui all'art. 640-ter cod. pen., in quanto si tratta di reati diversi: la frode informatica postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica.

## PISHING- 640 ter e 615 quater c.p.?

L'operazione può avvenire tramite server stranieri.

Una mail segnala improbabili controlli o vincite e induce ad entrare nel sito della Banca o delle Poste e reindirizza su un server straniero clone di quello ufficiale, dove viene chiesto di digitare le proprie credenziali.

E' davvero un artificio o un raggio?

# IL “FENOMENO” E-BAY .... ancora

Attività poste in essere presentandosi:

- con un account “ falso”
- con un account “rubato”

Il “furto” di identità potrebbe risalire a molto tempo prima dell’utilizzo dell’account : PROBLEMI di PROVA....  
su acquisizione dei log

## **IN CONCRETO.....**

**Account utilizzato indebitamente, impedendo l'accesso al titolare.**

**635 bis, 640 ter, 615 ter e quater c.p. ?**

**luogo di conseguimento del profitto SE L'AUTORE DEL FATTO E' LO  
STESSO**

**Account utilizzato indebitamente- art. 640 ter, 615 ter e quater c.p.**

**CONSUMAZIONE nel luogo di conseguimento del profitto**

**Se non accompagnato da utilizzo dell'account, l'accesso per "modificare"  
identificativi avviene nel luogo ove si trova il server**

**( 615 ter c.p. e 635 bis c.p. ?)**



# L'uso indebito di carte

Sez. 1, n. [37115](#) 2/10/2002 Ud. (dep. 05/11/2002 )

Rv. 222852

Costituisce indebita utilizzazione di carta di credito, ai sensi dell'art.12 del D.L.3 maggio 1991 n.143, convertito con modifiche in L.5 luglio 1991 n.197, **l'effettuazione attraverso la rete internet di transazioni**, previa immissione dei dati ricognitivi e operativi di una valida carta di credito altrui, acquisiti dall'agente fraudolentemente con il sistema telematico, nulla rilevando che il documento non sia stato nel suo materiale possesso.

*Sez. 2, Sentenza n. [32440](#) del 10/07/2003 Ud. (dep. 31/07/2003 ) Rv. 226259*

Integra il reato previsto dall'art. 12 d.l. 3 maggio 1991, n. 143, convertito nella legge 5 luglio 1991, n. 197, in tema di uso illecito di carte di credito o di pagamento, la condotta di chi procede a **ricaricare il cellulare utilizzando indebitamente codici relativi a carte di credito telefoniche** fraudolentemente sottratte da altri a chi le deteneva legittimamente, dovendosi ritenere che, ai sensi del citato art. 12, la scheda prepagata sia un "documento analogo" alle carte di credito o di pagamento, che abilita alla prestazione dei servizi telefonici

La S.C. esclude **la ricettazione, l'accesso abusivo ad un sistema informatico, la detenzione abusiva di codici di accesso a sistemi informatici e la frode informatica.**

## IN CONCRETO....

**Il soggetto che ha violato un p.c. e comunque acquisito o generato i dati di una carta NON coincide con il beneficiario dell'utilizzo. E di cosa risponde il beneficiario?**

- **ricettazione ?**
- **incauto acquisto ?**
- **concorso nell'art. 55, IX co., d.lgs 231/2007?**

**Problemi di prova dell'elemento soggettivo  
E' indispensabile iscrivere il beneficiario ???  
Analogie con ricettazione assegni.**

**Il reato – se esiste- per tale soggetto si consuma nel luogo di conseguimento del profitto ( dimora beneficiario): NON nel luogo della condotta (utilizzo dati carta) ma in quello di ricezione del pagamento.**

**Si può presumere in tutti i casi una violazione dell'art 615 quater c.p. con conseguente spostamento della competenza sulla Procura distrettuale ?**

**E in caso positivo, il reato si deve presumere consumato presso il luogo di residenza/dimora della p.o. ?**

**Verosimilmente NO**

## **IL RICICLAGGIO**

**Dopo l'acquisizione dei dati di un conto/ carta on line, viene richiesto a terzi di "girare" su conti esteri somme trasmesse per via telematica, a fronte di una commissione**

- **buona fede del terzo**
- **se NON è credibile, il reato si consuma nel luogo ove tale soggetto "pulisce" la somma disponendo un bonifico all'estero.**

**Competenza distrettuale solo se v'è prova di un reato informatico; no se il presupposto è l'art. 55 d. lgs. 231/2007**

# I REATI DI “EVENTO”

**Danneggiamento informatico, attentato ad  
impianti di pubblica utilità, accesso abusivo**

**Il luogo di consumazione coincide con quello del  
danno ( 635 bis c.p.) o dell'accesso ( 615 ter  
c.p.)**

## I REATI DI “ COMUNICAZIONE”: la diffamazione

*Sez. 5, n. [25875](#) del 21/06/2006 Ud. (dep. 25/07/2006 ) Rv.  
234528*

La diffamazione, che è reato di evento, si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa e dunque, nel caso in cui frasi o immagini lesive siano state immesse sul web, **nel momento in cui il collegamento viene attivato.**

*Sez. 5, Sentenza n. 16262 del 04/04/2008*

*Ud. (dep. 17/04/2008 ) Rv. 239832*

Ai fini dell'integrazione del delitto di diffamazione si deve presumere la sussistenza del requisito della comunicazione con più persone **qualora il messaggio diffamatorio sia inserito in un sito internet** per sua natura destinato ad essere normalmente visitato in tempi assai ravvicinati da un numero indeterminato di soggetti, quale è il caso del giornale telematico, analogamente a quanto si presume nel caso di un tradizionale giornale a stampa, **nulla rilevando l'astratta e teorica possibilità che esso non sia acquistato e letto da alcuno**



*Sez. 2, Sentenza n. [36721](#) del 21/02/2008*  
*Ud. (dep. 25/09/2008 ) Rv. 242085*

**Il reato di diffamazione consistente nell'immissione nella rete Internet di frasi offensive e/o immagini denigratorie, deve ritenersi commesso nel luogo in cui le offese e le denigrazioni sono percepite da più fruitori della rete, pur quando il sito "web" sia registrato all'estero.**

Sez. 5, n. [4741](#) del 17/11/2000 Cc. (dep. 27/12/2000 ) Rv. 217745

Il giudice italiano è competente a conoscere della diffamazione compiuta mediante l'inserimento nella rete telematica (internet) di frasi offensive e/o immagini denigratorie, anche nel **caso in cui il sito web sia stato registrato all'estero** e purché l'offesa sia stata percepita da più fruitori che si trovino in Italia; invero, in quanto reato di evento, la diffamazione si consuma **nel momento e nel luogo in cui i terzi percepiscono la espressione ingiuriosa.**

Nel caso in cui l'offesa venga arrecata tramite internet, l'evento appare temporalmente, oltre che concettualmente, ben differenziato dalla condotta: *“in un primo momento, si avrà l'inserimento "in rete", da parte dell'agente, degli scritti offensivi e/o delle immagini denigratorie, e, solo in un secondo momento (a distanza di secondi, minuti, ore, giorni ecc.), i terzi, connettendosi con il "sito" e percependo il messaggio, consentiranno la verifica dell'evento. “*

## **Cassazione, Sezione Terza Civile, ordinanza n.6591/2002**

In materia civile il luogo rilevante, ai fini del sorgere dell'obbligazione risarcitoria da fatto illecito non è il luogo dell'evento illecito ma **il luogo del danno conseguente** ( o se si vuole del successivo evento di danno) , da identificarsi nel luogo di domicilio dell'attore che assume di aver subito danni patrimoniali e danni morali dalle espressioni, assunte come offensive ed attribuite al convenuto nell'ambito di newsgroup posto in Internet

## ... MINACCE e simili

Lo strumento telematico si presta ad assicurare la possibilità di porre in essere qualsiasi forma di illecito che preveda forma di “dichiarazione” o “comunicazione” nell’ambito della fattispecie:

- minacce - art 612 c.p.
- obbligare taluno a “fare, tollerare o omettere qualche cosa” ( art 610 cp),
- costringere altri a “commettere un fatto costituente reato” ( art 611 cp)
  - ottenere un ingiusto profitto ( art 629 cp)
- esercitare arbitrariamente per proprie ragioni ( art 393 cp)
  - ATTI PERSECUTORI art 612 bis c.p.

**il reato si consuma nel luogo di percezione  
delle minacce o di conseguimento del  
profitto (estorsione)**

## .... INGIURIE

**Equiparate alla comunicazione “via lettera”**

**consumazione nel luogo di “ricezione” del  
messaggio**

# I REATI DI CONDIVISIONE

Sez. 3, n. [8296](#) del 02/12/2004 Cc. (dep. 03/03/2005 ) Rv. 231244

In riferimento all'ipotesi delittuosa di distribuzione, divulgazione o pubblicizzazione, anche per via telematica, di materiale pedo-pornografico, previsto dall'art. 600-ter, comma terzo, cod. pen., il **luogo di consumazione del reato coincide con il luogo nel quale è stato digitato il comando di invio delle foto per via internet.**

Tale momento corrisponde al momento di perfezionamento della fattispecie, ossia **all'immissione nella rete** del materiale fotografico illecito, a disposizione dei potenziali destinatari.

Sez. 3, n. [11169](#) del 07/11/2008 Ud. (dep. 13/03/2009 ) Rv. 242992

Ai fini dell'integrazione del reato di cui all'art. 600 ter, comma terzo, cod. pen., la condotta di divulgazione di materiale pedopornografico che avvenga in via automatica mediante l'utilizzo di appositi programmi di scaricamento da "internet", che **ne consentano al tempo stesso la condivisione con altri utenti** (ad esempio il programma cosiddetto "eMule"), presuppone comunque che i "files" di cui si compone detto materiale **siano interamente scaricati e visionabili nonché lasciati nella cartella dei "files" destinati alla condivisione.**



Sez. 3, n. [33945](#) del 04/07/2006 Cc. (dep. 10/10/2006 ) Rv. 234772

È configurabile il concorso nel reato di abusiva diffusione, mediante internet, di immagini protette da diritto di esclusiva anche in capo al soggetto che, pur non avendole immesse in rete, abbia **inoltrato sul web, in epoca antecedente alla loro immissione ad opera di altri, informazioni sui collegamenti e sui programmi necessari alla loro visione, in tal modo agevolando la connessione e la loro indebita diffusione.**

Sequestro preventivo di due portali "web", attraverso i quali erano state illecitamente trasmesse in diretta via internet partite del **campionato di calcio italiano**, mediante connessione ad emittenti cinesi che, acquistato il diritto di diffonderle localmente dal titolare dell'esclusiva, avevano ritenuto di immettere in rete la trasmissione degli eventi sportivi.

Sez. 3, n. [23164](#) 8/6/2006 Cc. (dep. 05/07/2006 ) Rv. 234639

Il delitto di distribuzione, divulgazione o pubblicizzazione di materiale pornografico realizzato mediante lo sfruttamento di minori degli anni diciotto sussiste quando il materiale sia propagato ad un numero indeterminato di destinatari, come avviene con l'inserimento nella rete internet mediante il modello di comunicazione "peer to peer" di filmati aventi come oggetto esibizioni pornografiche da parte di minori di anni 18 ed anche di anni 14.

Sez. 3, n. 593 del 07/12/2006 Cc. (dep. 15/01/2007 ) Rv. 236071

Commette il delitto di divulgazione via internet di materiale pedo-pornografico previsto dal comma terzo dell'art. 600 ter c. p. e non quello di mera cessione dello stesso, prevista al comma quarto del medesimo articolo, **non solo chi utilizzi programmi di "file-sharing peer to peer", ma anche chi impieghi una "chat line", spazio virtuale strutturato in canali, nella quale un solo "nickname", necessario ad accedere alla cartella-immagini o video, venga utilizzato da più persone alle quali siano state rese note l'"username" e la "password"**, le quali possono in tal modo ricevere e trasmettere materiale pedo-pornografico; tale sistema rende possibile trasferire il materiale pedo-pornografico a molteplici destinatari e non si differenzia perciò dalla divulgazione vera e propria, sempre che risulti provata in capo all'agente **la volontà alla divulgazione**, come nel caso in cui la trasmissione sia stata reiteratamente rivolta a più persone.

*Sez. 3, n. 12372 del 28/01/2003 Cc. (dep. 17/03/2003 ) Rv. 224244*

Ai fini della configurabilità del reato di cui all'art.600 ter, comma 3, cod. pen. (distribuzione, divulgazione o pubblicizzazione del materiale pornografico minorile) non è sufficiente la cessione di detto materiale a singoli soggetti ma occorre che esso sia propagato ad un numero indeterminato di persone.

Non è sufficiente quindi il mero utilizzo della rete internet - essendo comunque necessario che **l'offerta sia diretta ad un numero indeterminato di persone.**

**Ove** l'offerta sia destinata a persone determinate, sussiste la più lieve ipotesi di cui all'art.600-ter, comma 4, cod. pen., indipendentemente dall'uso o meno del mezzo telematico.

Occorre accertare quale tipo di **connessione telematica sia utilizzata al momento della commissione del reato: se si tratta di connessione aperta, sussiste il reato più grave di cui all'art.600 ter, comma 3, cod. pen., mentre, nell'ipotesi di connessione riservata, sussiste il reato più lieve di cui all'art.600 ter, comma 4, cod. pen.**

## ..... ALTRE FORME DI CONDIVISIONE.....

Sez. 3, n. [15158](#) del 21/03/2006 Cc. (dep. 03/05/2006 ) Rv. 233929

**Le prestazioni sessuali eseguite in videoconferenza via web-chat, in modo da consentire al fruitore delle stesse di interagire in via diretta ed immediata con chi esegue la prestazione, con la possibilità di richiedere il compimento di determinati atti sessuali, assume il valore di prostituzione e rende configurabile il reato di sfruttamento della prostituzione nei confronti di coloro che abbiano reclutato gli esecutori delle prestazioni o che abbiano reso possibile i collegamenti via internet, atteso che l'attività di prostituzione può consistere anche nel compimento di atti sessuali di qualsiasi natura eseguiti su se stesso in presenza di colui che, pagando un compenso, ha richiesto una determinata prestazione al fine di soddisfare la propria libido, senza che avvenga alcun contatto fisico fra le parti.**

Sez. 3, n. [5728](#) 17/11/2004 Cc. (dep. 15/02/2005 ) Rv. 230834

Il trattamento dei dati personali, che non siano sensibili né abbiano carattere giudiziario, effettuato da **un soggetto privato per fini esclusivamente personali** è soggetto alle disposizioni del d.lgs 196/2003 solo se i dati siano destinati ad una comunicazione sistematica o alla diffusione ed è in tal caso subordinato al consenso dell'interessato, a meno che il trattamento riguardi dati provenienti da pubblici registri od elenchi conoscibili da chiunque.

Aver comunicato ad alcuni "provider" le generalità, l'indirizzo, ivi compreso quello di posta elettronica, il numero di telefono e il codice fiscale di una persona senza il suo consenso, al fine di aprire un sito internet e tre nuovi indirizzi di posta elettronica a nome di tale persona, **non integra il reato di cui all'art. 167, comma primo D.Lgs. n. 196 del 2003.**

Grazie....