

Diritto ed economia delle nuove tecnologie  
Collana a cura di Daniele Minotti

1

# Diritto e società dell'informazione

*Riflessioni su informatica giuridica e diritto dell'informatica*

Circolo dei Giuristi Telematici  
Atti del Convegno di Grosseto 16/17 gennaio 2004

ottorino agati  
giuseppe bellazzi  
manuele bellonzi  
giuseppe campanelli  
maurizio castagno  
emmanuele cavanna  
nadina foggetti  
francesca romana fuxa sadurny  
giovanni battista gallus  
carmelo giurdanella  
elio guarnaccia  
laura lecchi  
andrea lisi  
angelo giuseppe orofino  
massimiliano pappalardo  
marco pepe  
marco pierani  
marco quadrelli  
giuliana romualdi

prefazione di daniele minotti

NYBERG EDIZIONI - MILANO

ISBN 88-901299-3-X

TUTTE LE COPIE DEVONO RECARE IL CONTRASSEGNO DELLA  
SIAE

© Copyright 2005 Nyberg S.r.l. - Milano - Tutti i diritti riservati. È consentita la riproduzione o fotocopia solo nei limiti stabiliti dalla legislazione vigente. La traduzione, l'adattamento totale o parziale, nonché la memorizzazione elettronica, sono riservati per tutti i Paesi.

---

Tipografia Copy & Photo S.r.l., via Caruso 2, 20133 Milano

## SOMMARIO

Prefazione .....	9
------------------	---

<b>Il programma del Convegno.....</b>	<b>11</b>
---------------------------------------	-----------

Ottorino Agati

<b>§ La configurabilità del dolo eventuale nel reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 <i>quinquies</i> c.p.).....</b>	<b>15</b>
---	-----------

Premessa .....	15
----------------	----

1. Sui crimini informatici .....	15
----------------------------------	----

2. L'art. 615 <i>quinquies</i> c.p. ....	17
--	----

2.1. Danneggiamento di un sistema informatico (art. 615 <i>quinquies</i> c.p.) .....	18
--	----

2.2. Bene giuridico .....	19
---------------------------	----

2.3. Oggetto materiale della condotta .....	19
---	----

2.4. Condotta .....	20
---------------------	----

2.5. Elemento psicologico .....	21
---------------------------------	----

2.6. Questioni.....	22
---------------------	----

2.7. È configurabile un dolo eventuale nell'art. 615 <i>quinquies</i> c.p.?..	22
---	----

2.8. La questione, ancora aperta, della "compatibilità" del dolo eventuale nel caso di delitto tentato (art. 56 c.p.).....	24
--	----

3. Conclusioni.....	25
---------------------	----

Giuseppe Campanelli

<b>§ La giurisprudenza della Corte di Cassazione in tema di "truffa informatica" .....</b>	<b>27</b>
--	-----------

1. Il dato codicistico .....	27
------------------------------	----

2. La giurisprudenza di legittimità .....	29
---	----

2.1. Sentenze n. 3065 e 3067 del 4.10.1999.....	29
---	----

2.2. Sentenza n. 32440 del 18 luglio 2003 .....	31
---	----

3. Nomen juris e tutela della privacy .....	34
---	----

Giovanni Battista Gallus

<b>§ L. 633/1941, d.lgs. 68/2003 e "Decreto Urbani": un'ipotesi ricostruttiva .....</b>	<b>37</b>
---	-----------

1. Il fenomeno del <i>peer to peer</i> .....	37
--	----

1.1. Il fenomeno del <i>peer to peer</i> .....	38
--	----

2. La disciplina positiva .....	39
---------------------------------	----

2.1. Mero <i>download</i> di <i>files</i> : quali sanzioni? .....	40
---	----

2.2. Profilo sanzionatorio del <i>file sharing</i> .....	41
3. Il decreto Urbani .....	44
3.1. Le modifiche alle sanzioni introdotte dal d.l. 72/2004 .....	45
3.2. La legge di conversione e la disciplina risultante .....	47

Emanuele Cavanna

**§ Diffamazione e Internet: la necessità di una normativa specifica .... 51**

Nadina Foggetti

**§ Ipotesi di criminalità informatica transnazionale: profili di diritto applicabile al caso concreto. Problematiche attuali ed eventuali prospettive future. .... 61**

1. Ipotesi di attacco a sistema informatico compiuto in territorio svizzero ai danni di utenti italiani. Cenni ai dati tecnici.....	61
2. Profili di diritto applicabile. Applicazione della normativa italiana. ....	65
3. Punibilità del reato nell'ambito della giurisdizione italiana.....	69
3.1. Presupposti per l'efficacia della legge penale italiana nello spazio.....	69
3.2. Applicabilità del principio di territorialità.....	72
3.3. Applicabilità del principio della difesa. ....	74
4. Applicazione del diritto penale svizzero. ....	76
4.1. Segue: l'applicazione del diritto svizzero. ....	79
5. La risposta europea ed internazionale al problema della criminalità informatica transfrontierana.....	82
5.1. Segue: la risposta europea al problema della criminalità informatica e la scelta dello strumento penale. ....	85

Laura Lecchi

**§ La disciplina delle comunicazioni commerciali secondo il d.lgs. 70/03 .....**

1. Premessa .....	91
2. La nozione di comunicazione commerciale.....	92
3. L'art. 8 del d.lgs. 70/03 .....	93
4. Segue: i progenitori dell'art. 8 d.lgs. 70/03 .....	94
5. Segue: considerazioni.....	95
6. Cenni sul direct marketing e l' e-mail marketing.....	96
7. La disciplina delle uce - unsolicited commercial e-mail - o comunicazioni commerciali non sollecitate, ex art. 9 d. lgs. 70/03 .....	97
8. Le tipologie di <i>opt in</i> .....	102

Giuliana Romualdi

**§ La tutela del cyber consumer: la risoluzione stragiudiziale delle controversie per via elettronica. La prospettiva italiana. .... 105**

1. Premessa. La tutela del cyber consumer nel d.lgs. n. 70/03. .... 105
2. Le On line Disputes Resolution. La situazione italiana. .... 109
3. Vantaggi della conciliazione on-line. Conclusioni. .... 111

Marco Pepe

**§ La comunicazione via Internet. Casi pratici e profili giuridici. .... 115**

1. Profili sociologici ..... 115
  - 1.1. Premessa ..... 115
  - 1.2. Evoluzione della comunicazione: dalla tradizione orale al computer. .... 117
  - 1.3. La realtà virtuale ..... 119
  - 1.4. Le reti di comunicazioni ..... 121
  - 1.5. La comunicazione nella rete ..... 122
  - 1.6. La “ persona “ in rete ..... 124
  - 1.7. Cooperazione e gratuità ..... 125
  - 1.8. Le Comunità Virtuali ..... 126
2. Internet e la protezione dei diritti costituzionali. Casi e giurisprudenza ..... 128
  - 2.1. Tendenze della giurisprudenza ..... 128
  - 2.2. - Il diritto di libertà informatica - la giurisprudenza USA. .... 128
  - 2.3. Differenti applicazioni tra la giurisprudenza negli USA e la giurisprudenza Europea. .... 132
  - 2.4. La tutela Costituzionale in Italia e l’art. 10 della Convenzione dei diritti dell’Uomo. Legislazione italiana a tutela della libertà delle comunicazioni. .... 133
  - 2.5. Alcuni Casi particolari ..... 134
    - 2.5.1. I Newsgroup ..... 134
    - 2.5.2. La Mailing List ..... 135
    - 2.5.3. La posta elettronica. .... 135
  - 2.6. Il diritto di critica. .... 136
    - 2.6.1. La giurisprudenza italiana sul diritto di critica. .... 140
  - 2.7. Conclusioni. .... 143

Andrea Lisi

**§ Il documento informatico nel commercio elettronico internazionale: e-mail e “accessi riservati” alla conquista di un’autonoma esistenza giuridica ..... 145**

1. Il documento informatico nel commercio elettronico internazionale .....	145
2. <i>Segue</i> : L'e-mail è quindi "forma scritta"? .....	153
3. <i>Segue</i> : Le altre conferme nella legislazione italiana e europea .....	159
4. <i>Segue</i> : Ultime novità legislative in Europa e Italia .....	161
5. <i>Segue</i> : E-mail, documento informatico, Id, Pw e firme elettroniche leggere .....	164
6. <i>Segue</i> : Conclusioni: registrazione nella personal zone e firma elettronica leggera .....	168

Marco Pierani

### **§ Concorrenza nella banda larga, dove sta l'interesse del consumatore?**

.....	173
1. Il mercato della banda larga in Europa .....	173
1.1. Pratiche abusive da parte degli incumbents .....	174
2. La situazione in Italia .....	175
2.1. Recenti sviluppi .....	176
2.2. Dolenti Note .....	177
3. Concorrenza e interessi del consumatore .....	177
3.1. Il ruolo delle Authorities .....	178
3.2. Il ruolo del Governo .....	180
4. Concorrenza nei contenuti .....	180
5. Conclusioni .....	181

Giuseppe Bellazzi

### **§ Uso e abuso dei sistemi informatici aziendali da parte dei dipendenti e responsabilità del datore di lavoro**

.....	183
1. Uno sguardo d'insieme .....	183
2. Tipologie di responsabilità .....	185
2.1. La responsabilità civile .....	185
3. La responsabilità penale .....	186
4. La responsabilità "amministrativa" .....	188
5. Le ipotesi di illecito .....	190
5.1. Le frodi .....	191
5.2. Le offese all'onore alla reputazione e all'integrità personale ..	192
5.3. La tutela dell'ambiente di lavoro .....	193
5.4. La diffusione indebita di informazioni di natura economica o aziendale .....	194
5.5. Violazioni della proprietà intellettuale .....	194
5.6. I reati 'informatici' .....	195
5.7. Il trattamento illecito dei dati personali .....	196

6. Quali contromisure?.....	198
Massimiliano Pappalardo	
<b>§ Profili giuridici del "linking" .....</b>	<b>199</b>
1. Introduzione.....	199
2. La liceità del <i>linking</i> .....	200
3. Il surface linking .....	201
4. Il deep linking .....	203
5. <i>Deep linking</i> e concorrenza sleale.....	204
6. <i>Segue</i> : due casi italiani.....	206
7. <i>Linking</i> e diritto d'autore .....	208
8. <i>Linking</i> e banche dati.....	210
Maurizio Castagno	
<b>§ La realizzazione di opere multimediali. problematiche giuridiche connesse .....</b>	<b>213</b>
1. Definizione di opera multimediale .....	213
2. La realizzazione di un'opera multimediale.....	214
3. Il contratto di licenza di riproduzione e commercio .....	214
3.1. L'oggetto del contratto di licenza di riproduzione e commercio .....	214
3.2. Le principali clausole del contratto di licenza di riproduzione e commercio .....	216
4. Il software gestionale .....	217
5. Ripartizione dei diritti .....	217
6. Conclusioni.....	218
Angelo Giuseppe Orofino	
<b>§ Informatica ed attività amministrativa.....</b>	<b>219</b>
1. Premessa. ....	219
2. Le ragioni dell'informatizzazione dell'attività amministrativa e l'attenzione del legislatore. ....	221
3. L'automazione amministrativa. ....	224
4. L'attività in forma elettronica. ....	230
4.1. La pubblicazione di atti amministrativi in Rete.....	239
4.2. La comunicazione individuale via e-mail. ....	241
5. Conclusioni.....	248
Carmelo Giurdanella ed Elio Guarnaccia	
<b>§ Gli appalti pubblici elettronici nella Direttiva 2004/18/CE.....</b>	<b>251</b>

1. Introduzione. L'utilizzo di strumenti informatici e telematici nelle procedure d'appalto secondo la nascente normativa europea. ....	251
2. I Sistemi Dinamici di Acquisizione .....	252
2.1. Nozione di sistema dinamico di acquisizione .....	252
2.2. Istituzione .....	253
2.3. Meccanismo di funzionamento .....	254
3. Comunicazioni .....	255
3.1. Principi generali .....	255
3.2. Specifiche tecniche dei mezzi di comunicazione .....	256
3.3. Regole applicabili alle domande di partecipazione .....	256
4. Contenuto dei verbali di gara e di aggiudicazione .....	257
5. Aste elettroniche .....	258
5.1. Nozione .....	258
5.2. Contenuto del capitolato d'oneri dell'asta elettronica .....	258
5.3. Svolgimento .....	259
5.4. Aggiudicazione .....	259
6. Accordi quadro .....	260
6.1. Definizione .....	260
6.2. Funzionamento .....	260
7. Bandi e avvisi di gara in Rete .....	260
8. Conclusioni .....	261

Francesca Romana Fuxa Sadurny

<b>§ Accesso ai documenti amministrativi e tutela della riservatezza alla luce del DPR n. 445/2000.....</b>	<b>263</b>
1. Diritto di accesso ai documenti amministrativi .....	263
2. Diritto di accesso ai documenti e tutela della riservatezza alla luce del d.lgs. 196/2003 e del DPR 445/2000 .....	266

Manuele Bellonzi

<b>§ Mediazione amministrativa telematica: l'esperienza del difensore civico virtuale .....</b>	<b>273</b>
---	------------

Marco Quadrelli

<b>§ La tutela del data base degli elenchi abbonati ai servizi telefonico e internet.....</b>	<b>283</b>
1. La normativa sulle banche dati. Cenni generali e indicazione dei problemi.....	283
2. I problemi connessi al caso degli elenchi di abbonati ai servizi telefonici.....	287

a) Titolarità del diritto d'autore, diritto di esclusiva ed alle sue limitazioni e diritto esclusivo di utilizzazione economica nei tipici modi di utilizzazione di banca dati .....	287
b) il diritto sui generis .....	288
c) La tutela penale (lo specifico caso della duplicazione abusiva degli elenchi del telefono) .....	293
d) Il concetto di creatività (nella compilazione degli elenchi telefonici) .....	296
3. La distribuzione in forma elettronica dell'elenco generale degli abbonati .....	297
3.1. La vigenza del diritto di esclusiva dell'Amministrazione dello Stato (artt.287 e 288 D.p.r. 29.3.1973 n. 156) ed il suo superamento .....	298
3.2. Il quadro normativo .....	301
3.3. Le regole e le modalità organizzative per la realizzazione e l'offerta di un servizio di elenco telefonico generale.....	302
3.3.1. La base dati elenco abbonati .....	308
3.3.2. Il servizio di elenco telefonico generale .....	312
3.3.3. Accordi quadro e informativa privacy .....	312
3.3.4. La distribuzione in forma elettronica dell'elenco generale degli abbonati e l'analisi dei costi e dei benefici dell'inserimento di tale distribuzione nel servizio universale.....	314
4. Conclusioni.....	315



## Prefazione

L'informatica giuridica e il diritto dell'informatica sono, oramai, divenuti temi quotidiani per i giuristi. O, almeno, dovrebbe essere così perché, pur tenuto conto della proverbiale avversione di coloro che provengono da un formazione giuridica, è, oggi, letteralmente improbabile non incappare, professionalmente, in casi che non presentino profili tecnici.

D'altro canto, al nostro tempo, la tecnologia è indispensabile anche per il giurista che vuole essere aggiornato, dunque professionalmente competitivo. Si pensi alle banche dati, off-line e on-line, che sempre più sostituiscono la carta anche per gli indubbi vantaggi in termini di produttività.

Il giurista, dunque, deve avere sufficiente dimestichezza con le nuove tecnologie sia per comprendere (al di là di consulenze delle quali, comunque, non sarebbe corretto fare a meno) su cosa sta lavorando, sia per poter fruire dei nuovi canali di informazione.

Sulla base di queste considerazioni, nel 1998 nasceva, primissimo tra i sodalizi del genere, il Circolo dei Giuristi Telematici ([www.giuristitelematici.it](http://www.giuristitelematici.it)), fondato da Francesco Brugaletta, Luca Ramacci e Giorgio Rognetta, sviluppatosi nella forma della mailing list erede di altre iniziative e dedicata alla discussione sui citati temi.

Quest'anno, dunque, ricorre il settimo anniversario della nascita del Circolo, in una storia, come detto, passata per un'intensa attività all'interno di una vivace ed informale mailing list - non per questo meno ricca di contributi di alto livello - ma anche per tre convegni che hanno coinvolto numerosi studiosi della materia.

Dal convegno pisano del novembre 2000, si è giunti al più recente incontro di Otranto tenutosi l'8 e il 9 ottobre 2004, passando per l'evento di Grosseto dai cui lavori è stata tratta questa pubblicazione.

La collettanea, volutamente costruita lasciando agli Autori - alcuni già molto noti, altri emergenti, ma tutti appartenenti al Circolo - la massima libertà in ordine alla scelta del tema, è il frutto anche della preziosa opera di coordinamento di Stefano Aterno (diritto penale), Giuseppe Nicosia (insostituibile padrone di casa) e Giorgio Rognetta (diritto civile e dell'impresa), Carmelo Giurdanella e Angelo Giuseppe Orofino (diritto amministrativo), non meri "chairman" delle rispettive sezioni, ma attivi "provocatori" di discussioni e riflessioni.

All'interno delle tre ideali sezioni non è stato, però, possibile limitare l'approfondimento nei confini delle singole branche. Molto spesso, infatti, è realmente arduo scrivere del diritto dell'informatica

limitandosi, ad esempio, al diritto civile, essendo presenti, al contrario forti contaminazioni interdisciplinari, specie quando ci si trova ad affrontare materie già organizzate in Testi Unici.

I temi affrontati sono, comunque, di estrema attualità, debitamente aggiornati con le eventuali novità presentatesi dopo il convegno e prontamente inserite per la realizzazione del volume.

Giusto per fare alcuni esempi, nella sezione penale si è trattato del decreto “Urbani” e della criminalità informatica transnazionale; in quella civile e dell’impresa, del documento informatico e delle responsabilità per abuso di mezzi informatici in ambito aziendale; in quella di diritto amministrativo, infine, di appalti elettronici e di accesso ai documenti amministrativi.

Il tutto, sempre per la libera scelta degli Autori, in alcuni casi mantenendo uno stile più discorsivo e più affrancato dalla necessità di corpose note giurisprudenziali e di dottrina, in una ideale riproduzione delle relazioni effettivamente tenutesi al convegno.

Non resta dunque che riservare un po’ di tempo alla lettura, magari ripromettendosi di approfondire e aggiornarsi partecipando alla mailing list del Circolo dei Giuristi Telematici.

Daniele Minotti  
daniele@minotti.net

## **Il programma del Convegno**

### **Diritto e società dell'informazione**

*Riflessioni su informatica giuridica e diritto dell'informatica*

Grosseto, 16-17 gennaio 2004

Sala delle contrattazioni - Camera di Commercio, Industria, Artigianato, Agricoltura - Via Cairoli, 10

### **Venerdì, 16 gennaio 2004**

Ore 9.00 - 13.00

*Sezione Prima: Diritto Penale*

Coordinano: avv. Stefano Aterno, Foro di Roma - avv. Daniele Minotti, Foro di Genova

Il reato di accesso abusivo a sistema informatico tra reato di danno e reato di pericolo

- *Avv. Stefano Aterno. Foro di Roma*

- *Avv. Daniele Minotti. Foro di Genova. Studio Legale Minotti. Curatore di Penale.it*

La configurabilità del dolo eventuale nel reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)

- *Avv. Otto Agati. Foro di Palermo. Redazione di CittadinoLex*

“Truffa” informatica: orientamenti giurisprudenziali di legittimità

- *Avv. Giuseppe Campanelli. Foro di Roma*

L. 633/1941, d.lgs 68/2003 e peer to peer: un'ipotesi ricostruttiva

- *Avv. Giovanni Battista Gallus. Foro di Cagliari. LL.M. Master of Laws. Dottore di ricerca*

Diffamazione e Internet: la necessità di una normativa specifica

- *Avv. Emanuele Cavanna. Foro di Roma*

Indagini informatiche e tutela dell'indagato

- *Avv. Giovanna Vettori. Foro di Bologna. Curatrice del sito della Camera Penale di Bologna*

Ipotesi di criminalità informatica transnazionale: problematiche attuali ed eventuali prospettive future

*Dott.ssa Nadina Foggetti. Foro di Bari. Studio Legale Orofino*

**Venerdì, 16 gennaio 2004**

Ore 15.00 - 19.30

*Sezione Seconda: Diritto Civile e dell'Impresa*

Coordinano: avv. Giuseppe Nicosia, Foro di Grosseto - avv. Giorgio Rognetta, Foro di Reggio Calabria

La tutela del consumatore nella società dell'informazione

*- Prof. Avv. Andrea Sirotti Gaudenzi. Foro di Forlì-Cesena. Professore a contratto presso l'Università degli studi di Padova. Direttore de Il Notiziario Giuridico Telematico*

La disciplina delle comunicazioni commerciali secondo il d.lgs. 70/2003

*- Avv. Laura Lecchi. Foro di Bologna. Curatrice di Cyberlex*

La tutela del cyber consumer: la risoluzione stragiudiziale delle controversie per via elettronica

*- Dott.ssa Giuliana Romualdi. Dottoranda di ricerca presso l'università di Bologna. Autrice nella collettanea La via della conciliazione. Vice Segretario della Camera Arbitrale e di Conciliazione di Grosseto*

Commercio elettronico e fiscalità internazionale applicata

*- Prof. Giampaolo Corabi. Università ITBA-Buenos Aires. Studio Legale Sutti*

Uso delle comunicazioni commerciali nelle professioni regolamentate... riguarda anche gli avvocati?

*- Dott. Marco Pistis. Foro di Milano. Studio Abbatascianni e Associati*

La comunicazione via Internet. Casi pratici e profili giuridici

*- Avv. Marco Pepe. Foro di Roma*

Tra Codice della Privacy e firma elettronica il trattamento dei dati personali su Internet rimane un rebus: prove tecniche sull'acquisizione del consenso telematico

*- Avv. Andrea Lisi. Foro di Lecce. Studio Associato D&L. Vice Presidente Centro Studi & Ricerche SCiNT*

Le firme elettroniche nell'organizzazione imprenditoriale

– *Avv. Massimiliano Nicotra. Foro di Roma*

Aspetti problematici dell'esecuzione di provvedimenti giudiziari concernenti un sito Web

– *Avv. Luca-Maria de Grazia. Foro di Frosinone. Si occupa da tempo delle problematiche connesse ai rapporti tra Internet, reti e diritto*

Concorrenza nella banda larga, dove sta l'interesse del consumatore?

– *Avv. Marco Pierani. Relazioni Esterne Istituzionali Altroconsumo*

Uso e abuso dei sistemi informatici aziendali da parte dei dipendenti e responsabilità del datore di lavoro

– *Avv. Giuseppe Bellazzi. Direzione Affari Legali di Banca Intesa*

Profili giuridici del linking

– *Avv. Massimiliano Pappalardo. Foro di Como*

La realizzazione di opere multimediali. Problematiche giuridiche connesse

– *Dott. Maurizio Castagno. Foro di Genova. Studio Legale Catania-Castagno*

I “creative commons” nell’esperienza statunitense

– *Avv. Giuseppe Nicosia. Foro di Grosseto*

**Sabato, 17 gennaio 2004**

Ore 9.30 – 13.00

*Sezione Terza: Diritto Amministrativo*

Coordinano: avv. Carmelo Giurdanella, Foro di Catania – avv. Angelo Giuseppe Orofino, Foro di Bari

Informatica ed attività amministrativa

– *Avv. Angelo Giuseppe Orofino. Foro di Bari. Studio Legale Orofino. Specializzato in scienze delle autonomie costituzionali presso l’Università di Bari. Comitato scientifico Csig*

Appalti pubblici elettronici: dalla pubblicazione del bando on-line all’aggiudicazione telematica

– *Avv. Carmelo Giurdanella. Amministrativista in Catania. Studio Legale Giurdanella & Associati. Coordinatore didattico Corso Alta Formazione in Diritto delle nuove tecnologie, Università Cattolica del Sacro Cuore. Chairman DAE*

– *Avv. Elio Guarnaccia. Foro di Catania. Studio Legale Giurdanella & Associati*

L'appalto pubblico ad oggetto informatico nella più recente giurisprudenza amministrativa

– *Avv. Carmelo Giurdanella. Amministrativista in Catania. Studio Legale Giurdanella & Associati. Coordinatore didattico Corso Alta Formazione in Diritto delle nuove tecnologie, Università Cattolica del Sacro Cuore. Chairman DAE*

– *Avv. Elio Guarnaccia. Foro di Catania. Studio Legale Giurdanella & Associati*

Open source nella pubblica amministrazione

– *Avv. Fabio Tommasi. Foro di Lecce. Studio Legale Tommasi*

L'accesso ai documenti amministrativi, l'accesso al trattamento dei dati personali: l'impatto delle nuove tecnologie

– *Avv. Francesca Romana Fuxa Sadurny. Foro di Roma*

Mediazione amministrativa telematica: l'esperienza del difensore civico virtuale

– *Dott. Manuele Bellonzi. Consulente Istituto Fisiologia Clinica-C.N.R. e S.S.S.U.P. Sant'Anna di Pisa. [Difesacivica.it](http://Difesacivica.it)*

Gli interventi pubblici di sostegno al settore del commercio elettronico

– *Dott. Francesco Di Biasi. Consulente legale d'impresa, Cesena*

Nuove tecnologie e rapporto tributario: prospettive e problemi

– *Avv. Antonino Attanasio. Foro di Forlì-Cesena*

La tutela del database degli elenchi abbonati ai servizi telefonico e Internet

– *Dott. Marco Quadrelli. Amministratore delegato e Legal Problem Solution Manager Ararat Service (Italia) S.r.l.*

Ottorino Agati<sup>1</sup>

## § La configurabilità del dolo eventuale nel reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 *quinquies* c.p.)

SOMMARIO: 1. Sui crimini informatici - 2. L'art. 615 *quinquies* c.p. 2.1 Danneggiamento di un sistema informatico 2.2 Bene giuridico 2.3 Oggetto materiale della condotta 2.5 Elemento psicologico 2.7 È configurabile un dolo eventuale nell'art. 615 *quinquies* c.p.? 2.8 La questione, ancora aperta, della "compatibilità" del dolo eventuale nel caso di delitto tentato (art. 56 c.p.) - 3. Conclusioni.

### Premessa

Il mio breve intervento sarà principalmente incentrato su due profili: uno, introduttivo, nel quale cercherò di tratteggiare quale sia la reale portata, ad oggi, dei cosiddetti **crimini informatici**; un secondo che riguarderà taluni aspetti penal processuali dell'art. 615 *quinquies* c.p. "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico" (introdotto, come è noto, dalla L. 547/1993), in particolare, se siano configurabili in questa fattispecie di reato il dolo eventuale e il tentativo del reato.

### 1. Sui crimini informatici

*Tra leggenda metropolitana e realtà*

Diciamo subito che il problema dei crimini informatici è, a mio parere, sopravvalutato dai più: a giudicare, infatti, dall'esperienza giurisprudenziale di questi ultimi anni in cui la diffusione di internet - e, quale "naturale" conseguenza, dei reati commessi per mezzo della rete -

---

<sup>1</sup> Avvocato, Foro di Roma, redazione di Cittadinolex..it

si è ampliata, l'**incidenza dei reati informatici** rispetto ai reati cosiddetti classici è scarsa e in percentuali ancora vicine al 3-4%.

I più accorti operatori del diritto si sono chiesti le motivazioni di questa incidenza così bassa che, soprattutto se confrontata con le notizie che appaiono sui giornali e sui media in genere, rende evidente una **contraddizione**.

Si osservi, peraltro, che - a parte una limitata nicchia di esperti - solamente quando sorge un problema si acquisisce consapevolezza dei pericoli insiti nella navigazione in rete.

Grave errore, però, sarebbe quello di generalizzare: è come se, adottando un esempio paradossale, - a fronte dell'omicidio di un soggetto colpito a morte a martellate affermassimo che il martello sia uno strumento pericoloso. Al contrario, il martello non è uno strumento pericoloso ma, se abusato, *veramente* diventa uno strumento pericoloso: lo stesso valga, fuor di metafora, per la rete che non è in sé stessa pericolosa, ma lo diventa se abusata in modo criminale potendo produrre dei seri danni. La stessa "esagerazione" la si riscontra in relazione al fenomeno degli hackers.

Allora con quali modalità e in quali occasioni sorgono i "guai"? Il problema risiede, soprattutto, nella **sicurezza interna**: recenti ricerche americane dimostrano come, su un ampio campione di aziende - il 40-50% delle quale aveva dei siti internet - è risultato che ben l'80% dei problemi avuti nel sistema provenivano dall'interno. È, peraltro, emerso che nei casi più gravi si trattava dei lavoratori stessi dell'azienda, i quali accedevano al sistema provocandone (più o meno dolosamente) una disfunzione o un danneggiamento; solo in una percentuale bassissima di casi, i problemi venivano dall'esterno - cioè si trattava di vere e proprie intrusioni informatiche.

Occorre allora, ragionevolmente, affidarsi alla **protezione dall'interno**. Le più grandi aziende si sono da tempo organizzate, hanno predisposto dei gruppi di lavoro che si occupano unicamente della protezione del sistema e di impedire l'accesso non autorizzati ai sistemi informatici rivelando e superando, in tale modo, uno dei problemi principali sorti nei primi anni di diffusione di internet.

Da tale breve e sintetica analisi discende che molti dei problemi in rete siano provocati dai **privati**: tutti noi con i nostri personal computer a casa o in ufficio subiamo regolarmente intrusioni esterne, le quali tuttavia, nella stragrande maggioranza dei casi, non producono alcun danno: proviamo, certo, un fastidio, ma raramente questo fastidio si traduce in danneggiamento dei dati immessi nel computer.

Va anche considerato che il privato talvolta si sente in qualche modo non protetto nel caso di attacchi dall'esterno.

Nel caso di esposti spesso l'Autorità avanza richiesta di archiviazione per l'impossibilità/inutilità di proseguire le indagini - dal momento che chi decide di attaccare il sistema informatico ha approfondite cognizioni tecniche e quindi in molti casi è virtualmente impossibile, o perlomeno molto difficile, riuscire con le attuali conoscenze a rintracciare i colpevoli di questo tipo di reati e, peraltro, il dispendio di risorse economiche ed umane è eccessivo rispetto all'effettivo danno subito dall'utente.

Ora vediamo di capire *cosa sono* i crimini informatici: intanto *non vi è una formale definizione* di crimine informatico. Possiamo, con l'ausilio della dottrina più attenta, solo abbozzare una definizione abbastanza ampia e quindi comprensiva di tutti gli elementi: è crimine informatico **quella condotta penalmente rilevante in cui il ricorso alla tecnologia informatica sia stato un fattore determinante per il compimento dell'atto.**

Di rilievo è la distinzione tra reati telematici veri e propri, caratterizzati dall'utilizzo di tecnologie informatiche, e crimini cosiddetti tradizionali attuati con il mezzo del sistema informatico.

Lo **stato della nostra legislazione**: il nostro legislatore è intervenuto in materia con la L. n. **547 del 23 dicembre 1993.**

Questa legge ha inserito alcuni articoli nel Codice Penale o specificato le condotte tradizionali. Nella relazione - che invito a leggere perché ricca di spunti di riflessione - sul disegno di legge n. 2773 vi è da parte del Ministro una spiegazione di questa scelta: si è evitato da parte del legislatore di inserire un titolo apposito nel codice penale e si è preferito invece inserire (con il sistema dei *ter, quater, quinquies...*) delle norme giustapposte su un tracciato già esistente. Tale tecnica, talvolta, determina all'utente una **mancata o errata comprensione**: avviene così che in alcuni casi questi reati vengano commessi anche inconsapevolmente a causa di una **dispersione o una cattiva (quando non errata) formulazione delle norme.**

## **2. L'art. 615 quinquies c.p.**

Entro, adesso, nello specifico della seconda parte della mia conversazione.

Si osservi che il legislatore ha affrontato direi in maniera incisiva la questione del danneggiamento di sistemi informatici pubblici e privati. In effetti, almeno due sono stati gli interventi di interesse: il primo attuato, come detto, dalla l. 547/1993 che ha introdotto diverse figure di reati perpetrati con il mezzo informatico e, in particolare, appunto l'art. 615 *quinquies* c.p.; il secondo attuato con la legge c.d. di tutela della privacy (la l. 675/96, oggi sostituita dal dlgs 30.6.2003 n. 196) e cioè con l'introduzione di specifiche sanzioni nel caso di omessa adozione – anche da parte dei privati – di misure necessarie alla sicurezza dei dati (v. artt. 31 ss. e 169).

## **2.1. Danneggiamento di un sistema informatico (art. 615 *quinquies* c.p.)**

*“Chiunque diffonde, comunica o consegna 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, è punito con la reclusione sino a due anni e con la multa sino a € 10.329.”*

*Questo articolo è stato aggiunto dall' art. 41 della L. 23 dicembre 1993. n. 547 recante modificazioni e integrazioni alle norme del codice penale e di procedura in tema di criminalità informatica.*

Procedibilità: ufficio; competenza: Tribunale monocratico; citazione diretta a giudizio.

Con tale disposizione – che non ritroviamo in molti altri ordinamenti – il nostro legislatore ha dotato il nostro ordinamento di un elemento in più nella lotta contro un fenomeno piuttosto insidioso e, per molti aspetti, dai contorni e dalle dimensioni “oscuri”.

Come è noto, infatti, l'aumento esponenziale dell'uso di internet e dello scambio di dati tra gli utenti (anche attraverso supporti magnetici o allegazioni ad *email*) o, ancora, il sempre maggiore desiderio di ricerca in rete hanno incrementato la diffusione di programmi contenenti virus. In questo campo, tra l'altro, come già in parte osservato si verifica un singolare fenomeno: una generale ritrosia alla denuncia del fatto all'Autorità.

Tale circostanza può trovare diverse spiegazioni: da un lato, allorché il sistema infettato dal virus abbia notevoli dimensioni (si pensi