

GIOVANNI ZICCARDI

## TELEMATICA GIURIDICA

Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto

(contributi di Silvia Bisi, Matteo Giacomo Jori, Pierluigi Perri, Daniele Pizzi, Cristina Rabazzi)

Giuffrè editore - Milano – 2005



Introduzione

### PARTE PRIMA - LE NUOVE TECNOLOGIE E LA LORO STORIA

#### Capitolo I - IL "GIURISTA - HACKER"

- 1.1. Hacking come conoscenza della tecnologia: l'approccio "meccanico" e il "giurista - hacker"
- 1.1.2. Il "giurista - hacker"
- 1.2. L'origine e l'evoluzione di un'"etica hacker"
- 1.3. Eric S. Raymond e il suo pensiero: i comportamenti
- 1.4. La programmazione
- 1.5. L'utilizzo di sistemi open source
- 1.6. Le attività
- 1.7. L'evoluzione dell'hacking
- 1.8. I moventi psicologici
- 1.9. L'Homebrew Computer Club

#### Capitolo II - IL PENSIERO INFORMATICO: STUDIOSI E TECNICI

- 2.1. L'evoluzione informatica e gli studiosi di riferimento
- 2.2. Lawrence Lessig e Creative Commons: una forma flessibile di copyright
- 2.3. L'attività di Eric S. Raymond e il concetto di open source
- 2.4. Richard Stallman e la Free Software Foundation: il software libero
- 2.5. Dennis Ritchie, Ken Thompson e il sistema operativo Unix
- 2.6. John Draper ("Captain Crunch") e l'hacking dell'hardware

- 2.7. Steve Wozniak e la Apple
- 2.8. Linus Torvalds e il sistema operativo Linux
- 2.9. John Perry Barlow e la Electronic Frontier Foundation
- 2.10. Jon Johansen e il caso giudiziario del DeCSS
- 2.11. Dmitry Sklyarov e Adobe
- 2.12. Ed Felten e il "pen felt hack"
- 2.13. Emmanuel Goldstein e il caso giudiziario "2600"
- 2.14. Johan Helsingius e penet.fi
- 2.15. Mark Abene ("Phiber Optik") e i Masters of Deception
- 2.16. Robert Morris e il primo worm di Internet
- 2.17. Kevin Mitnick: il "condor"
- 2.18. Kevin Poulsen: il "serial hacker"
- 2.19. Vladimir Levin: l'hacker russo
- 2.20. Ian Murphy
- 2.21. Karl Koch e il KGB

### Capitolo III - ELABORATORE ELETTRONICO, SUA EVOLUZIONE E MONDO GIURIDICO

- 3.1. La conoscenza della macchina
- 3.2. Il computer e la sua storia
  - 3.2.1. Le origini e i computer di "prima generazione"
  - 3.2.2. I computer di "seconda generazione"
  - 3.2.3. I computer di "terza generazione"
  - 3.2.4. I computer di "quarta generazione"
  - 3.2.5. L'era moderna
- 3.3. Il computer "stand alone"
  - 3.3.1. Il computer come insieme di hardware e software
  - 3.3.2. Il codice binario
  - 3.3.3. La CPU
  - 3.3.4. La RAM
  - 3.3.5. Le memorie di massa
  - 3.3.6. Le periferiche
- 3.4. Il computer collegato in rete

### Capitolo IV - IL CONCETTO DI RETE DI COMPUTER E IL GIURISTA

- 4.1. Il giurista e le reti di computer
- 4.2. Le tipologie di rete di computer e le caratteristiche essenziali
  - 4.2.1. La condivisione delle risorse
  - 4.2.2. La comunicazione
- 4.3. Le LAN
  - 4.3.1. L'architettura client/server
  - 4.3.2. Le cosiddette "topologie di rete"
- 4.4. Le WAN
- 4.5. Le reti wireless
- 4.6. La tecnologia Bluetooth e i collegamenti mobili
- 4.7. La Rete Nazionale della Pubblica Amministrazione

- 4.8. Le reti nei Tribunali
- 4.9. La rete nel processo civile telematico
- 4.9.1. Il progetto Polis
- 4.9.2. PolisWeb per gli avvocati

## Capitolo V - INTERNET E I SUOI SERVIZI PER IL GIURISTA: UN'INTRODUZIONE

- 5.1. Internet come strumento per il giurista
- 5.2. Le origini di Internet
- 5.3. Le tecnologie alla base di Internet
- 5.3.1. La rete delle reti
- 5.3.2. Gli indirizzi Ip e i domini
- 5.4. I servizi di Internet
- 5.5. La posta elettronica
- 5.6. FTP
- 5.7. I newsgroups
- 5.8. Le mailing lists
- 5.9. Il World Wide Web
- 5.10. Le chat
- 5.11. L'instant messaging
- 5.12. I nuovi servizi

## Capitolo VI - IL CLIENT, IL LINGUAGGIO DEL COMPUTER E I VARI SISTEMI OPERATIVI

- 6.1. Il computer del giurista
- 6.2. Il sistema operativo
- 6.3. I sistemi operativi proprietari
- 6.4. I sistemi operativi aperti
- 6.4.1. Il software open source per gli studi legali
- 6.5. Il client per il collegamento ad Internet e la sua configurazione tipica
- 6.5.1. La mobilità
- 6.5.2. Le prestazioni
- 6.5.3. La connettività
- 6.5.4. Il software

## Capitolo VII - IL GIURISTA AL COMPUTER

- 7.1. Il computer "ideale"
- 7.2. L'approccio corretto
- 7.3. La letteratura di riferimento
- 7.4. Il rapporto con Internet
- 7.5. Privacy e segretezza dei dati

## **PARTE SECONDA - UTILIZZARE LE TECNOLOGIE**

## Capitolo VIII - LA POSTA ELETTRONICA E LA POSTA ELETTRONICA CERTIFICATA

- 8.1. L'origine della posta elettronica
- 8.2. La posta elettronica tramite client
- 8.3. La posta elettronica via Web
- 8.4. I campi. La e-mail "per conoscenza"
- 8.5. La gestione corretta degli allegati
- 8.6. I virus via e-mail
- 8.7. L'origine della posta e il percorso: gli headers
- 8.8. Lo spamming e la posta non sollecitata
  - 8.8.1. Lo spamming
  - 8.8.2. Fare spam
  - 8.8.3. Difendersi dallo spam
- 8.9. La e-mail anonima
- 8.10. La riservatezza e i problemi di sicurezza nella posta elettronica
- 8.11. La firma della e-mail
- 8.12. Le truffe via e-mail
- 8.13. Il phishing
- 8.14. La posta elettronica certificata (PEC)
- 8.15. L'utilizzo della posta elettronica certificata
- 8.16. La sicurezza della posta elettronica certificata
- 8.17. I gestori della posta elettronica certificata
- 8.18. Il funzionamento della posta elettronica certificata

## Capitolo IX - L'UTILIZZO DELLE MAILING LISTS DA PARTE DEL GIURISTA

- 9.1. Le mailing lists
- 9.2. L'iscrizione a una mailing list
- 9.3. Il regolamento della mailing list
- 9.4. La creazione di una mailing list
- 9.5. La gestione dei messaggi della mailing list
  - 9.5.1. I software di gestione: un esempio
  - 9.5.2. Le liste moderate
  - 9.5.3. La gestione da parte degli iscritti
- 9.6. Le mailing lists giuridiche
- 9.7. Mailing lists giuridiche suddivise per argomento
- 9.8. Mailing lists giuridiche suddivise per operatori:

## Capitolo X - L'UTILIZZO DEI NEWSGROUPS DA PARTE DEL GIURISTA

- 10.1. I newsgroups
- 10.2. L'iscrizione a un newsgroup
  - 10.2.1. I newsservers
  - 10.2.2. Le gerarchie
  - 10.2.3. I manifesti
  - 10.2.4. I newsgroups moderati

- 10.2.5. Scelta del nickname e dell'e-mail associata
- 10.3. Consultare i newsgroups e "postare" i messaggi
  - 10.3.1. Prima di iniziare a "postare"
  - 10.3.2. Consultazione dei newsgroups tramite Web
  - 10.3.3. Utilizzo di un newsreader
  - 10.3.4. Impostazione di filtri
  - 10.3.5. I files binari
- 10.4. Creare un newsgroup
- 10.5. I newsgroups giuridici

## Capitolo XI - I SISTEMI DI MESSAGGISTICA, LA CHAT, I CONTATTI, IL FILE SHARING PER IL GIURISTA

- 11.1. IRC
  - 11.1.1. La nascita di IRC
  - 11.1.2. Le funzionalità di IRC
  - 11.1.3. Le modalità di interazione con IRC
  - 11.1.4. La sicurezza di IRC
  - 11.1.5. Il cattivo funzionamento di IRC
  - 11.1.6. I casi patologici di IRC e IRCwar: attacco DoS, Nuke, Takeover
- 11.2. ICQ
  - 11.2.1. La nascita di ICQ
  - 11.2.2. Il funzionamento di ICQ
  - 11.2.3. La sicurezza di ICQ
- 11.3. Gli altri sistemi di messaggistica istantanea
  - 11.3.1. Il funzionamento
  - 11.3.2. I sistemi più utilizzati
  - 11.3.3. I sistemi multi piattaforma
  - 11.3.4. Le chat
- 11.4. I sistemi di file sharing
  - 11.4.1. BitTorrent e WinMx
- 11.5. Le funzionalità di Skype

## **PARTE TERZA - LE INFORMAZIONI IN INTERNET**

### Capitolo XII - LA RICERCA DELLE INFORMAZIONI

- 12.1. La ricerca in Internet
- 12.2. Informazione ordinata e informazione disordinata
  - 12.2.1. L'organizzazione delle informazioni
- 12.3. L'informazione strutturata
  - 12.3.1. La ricerca su basi di dati
- 12.4. La ricerca libera sul Web
  - 12.4.1. I motori di ricerca per termini
  - 12.4.2. Le directory
  - 12.4.3. La ricerca orizzontale
- 12.5. Gli indici sistematici

## Capitolo XIII - IL WEB GIURIDICO

- 13.1. Nascita ed evoluzione del Web giuridico
- 13.2. I contenuti giuridici sul Web
  - 13.2.1. Riviste e periodici
  - 13.2.2. Raccolte e banche dati
  - 13.2.3. Siti istituzionali
  - 13.2.4. Altri siti di interesse giuridico
- 13.3. Alcuni siti indispensabili per il giurista
  - 13.3.1. Guide e strumenti di ricerca
  - 13.3.2. Riviste, periodici, portali
  - 13.3.3. Siti istituzionali
  - 13.3.4. Altri siti utili

## Capitolo XIV - CREARE IL PROPRIO SITO WEB: TECNOLOGIE E REGOLE

- 14.1. Il sito Web del professionista: nozioni di base
  - 14.1.1. Cos'è un sito web
  - 14.1.2. Tipologie di siti Web
  - 14.1.3. Finalità e scopi del sito web professionale
- 14.2. Come creare un sito web professionale
  - 14.2.1. Scegliere il nome e l'estensione di dominio
    - L'estensione del dominio.
    - Alcune Regole di Naming: tipo, numero dei caratteri e altri limiti.
  - Il significato del nome
  - Il valore commerciale
  - 14.2.2. Scegliere lo spazio web
  - 14.2.3. Note tecniche per acquisto e registrazione di nomi di dominio e spazio web
  - 14.2.4. Considerazioni di base su creazione e pubblicazione delle pagine web
- 14.3. Il fenomeno dei Blog
  - 14.3.1. I Blog
  - 14.3.2. Blog e siti web: analogie e differenze
  - 14.3.3. Come creare un Blog
- 14.4. I contenuti di un sito web professionale
  - 14.4.1. La presentazione dell'attività esercitata e dello studio legale
  - 14.4.2. Il contatto con il cliente
  - 14.4.3. Contenuti normativi, giurisprudenziali e dottrinali

## Capitolo XV - I nomi a dominio in Italia

- 15.1. Introduzione
  - 15.1.1. Gli indirizzi telematici
  - 15.1.2. Che cos'è un nome a dominio
- 15.2. Gli organi per la registrazione del nome a dominio in Italia
  - 15.2.1. La Registration Authority Italiana

- 15.2.2. La Naming Authority Italiana
- 15.3. La procedura di registrazione di un nome a dominio
  - 15.3.1. Il Registro ccTLD "it"
  - 15.3.2. La Commissione per le Regole e le Procedure Tecniche del Registro del ccTLD ".it"
  - 15.3.3. Le Regole per l'assegnazione di un nome a dominio
  - 15.3.4. I passi da seguire per una corretta registrazione
- 15.4. La modifica di un nome a dominio
- 15.5. Il trasferimento di un nome a dominio
- 15.6. la revoca di un nome a dominio assegnato
- 15.7. La sospensione di un nome a dominio
- 15.8. la contestazione e la risoluzione dei conflitti per i domini ".it"
  - 15.8.1. Procedura Arbitrale
  - 15.8.2. Procedura di riassegnazione

## **PARTE QUARTA - I COMPORAMENTI**

### Capitolo XVI - ETICA, TEORIE E LIBERTA' DEL CODICE

- 16.1. Etica e informatica
  - 16.1.1. Le regole e i principi
  - 16.1.2. Il digital divide
- 16.2. I codici etici nell'informatica
  - 16.2.1. L'Internet Ethic Code di ISEC
  - 16.2.2. L'ACM Code of Ethics and Professional Conduct
  - 16.2.3. Il Code of Professional Ethics di ISACA
- 16.3. L'etica hacker
  - 16.3.1. The Jargon file
  - 16.3.2. La "Legge di Linus"
- 16.4. Il codice libero e l'open source
  - 16.4.1. L'Open Source Definition
- 16.5. La "filosofia" del free software e la Free Software Foundation
  - 16.5.1. La GNU- General Public License

### Capitolo XVII - LA NETIQUETTE

- 17.1. Il "galateo" di Internet
- 17.2. I codici di autodisciplina
  - 17.2.1. Il Codice di Autoregolamentazione per i servizi Internet
  - 17.2.2. Il Codice del Ministero delle Poste e Telecomunicazioni
  - 17.2.3. Le regole generali di comportamento nel codice
  - 17.2.4. Gli organi
  - 17.2.5. Il Codice di deontologia e di buona condotta per i servizi telematici
  - 17.2.6. La carta delle garanzie di Internet
  - 17.2.7. Confronto tra le proposte di autoregolamentazione
- 17.3. La netiquette della Naming Authority Italiana

#### 17.4. La netiquette a livello internazionale

### Capitolo XVIII - INTERNET E DEONTOLOGIA FORENSE

#### 18.1. L'evoluzione della professione legale nell'era di Internet

18.1.1. La presenza in Internet di un numero elevato di potenziali clienti

18.1.2. La presenza di altri avvocati in Internet

18.1.3. La possibilità di discutere temi giuridici con probabili futuri clienti o con altri professionisti

18.1.4. L'accesso all'informazione giuridica e la velocità con cui è possibile scambiare i dati

18.1.5. Il costo irrisorio delle comunicazioni

#### 18.2. Internet e la deontologia professionale forense

18.2.1. La pubblicità sul Web dello studio legale: l'art. 17 del Codice Deontologico Forense

18.2.2. Il testo dell'articolo 17

18.2.3. Il commento all'art. 17 e i mezzi di comunicazione

18.2.4. Le informazioni

18.2.5. La libertà di informare e i suoi limiti

18.2.6. La segnalazione del sito all'Ordine

18.2.7. La consulenza online, o per via telematica

18.2.8. Il parere dell'Ordine di Milano

18.2.9. Il Consiglio Nazionale Forense e le consulenze online

#### 18.3. La professione legale e la deontologia forense in Europa

18.4. Il dovere di aggiornamento professionale

### Capitolo XIX - LE POLICIES DI SICUREZZA

19. 1. Policies e comportamenti

19.2. Esempio di security policy in tema di uso del personal computer aziendale e dei supporti magnetici

19.3. Esempio di security policy in tema di utilizzo della rete aziendale e Internet Access Policy

19.4. Esempio di security policy in tema di utilizzo della posta elettronica e gestione della casella e-mail aziendale

## **PARTE QUINTA - LA SICUREZZA**

### Capitolo XX - Introduzione alla crittografia per il giurista

20.1. La crittografia e il giurista

20.2. La crittografia simmetrica

20.3. Il DES (Data Encryption Standard)

20.4. La crittografia asimmetrica

20.5. L'algoritmo RSA

20.6. Altri algoritmi



- 20.7. Le funzioni hash unidirezionali
- 20.8. Gli algoritmi MD2, MD4 e MD5
- 20.9. L'algoritmo SHA-1

## Capitolo XXI - L'USO DI PGP DA PARTE DEL GIURISTA

- 21.1. Le origini
- 21.2. Perché usare PGP?
  - 21.2.1. La cifratura dei dati
  - 21.2.2. La firma digitale
- 21.3. Procedura di installazione
  - 21.3.1. Acquisto o download del software
  - 21.3.2. L'installazione sul sistema operativo
  - 21.3.3. Creazione della coppia di chiavi
    - a- Procedura semplificata
    - b- Procedura per esperti
  - 21.3.4. Salvare la propria chiave privata
  - 21.3.5. Pubblicare la propria chiave pubblica
- 21.4. Menu e proprietà
  - 21.4.1. Interfaccia principale
  - 21.4.2. PGPkeys
  - 21.4.3. Proprietà delle chiavi
- 21.5. Il funzionamento di PGP
  - 21.5.1. Cifrare
  - 21.5.2. Decifrare
  - 21.5.3. Firmare
  - 21.5.4. Verificare
  - 21.5.5. Esportare una chiave
  - 21.5.6. Importare una chiave
  - 21.5.7. Revocare una chiave
  - 21.5.8. Dichiarare una chiave valida
  - 21.5.9. Cercare una chiave
  - 21.5.10. Generare un archivio autodecifrante (SDA)
- 21.6. Plugin e opzioni per la posta elettronica
- 21.7. PGPdisk
  - 21.7.1. Introduzione a PGPdisk
  - 21.7.2. L'uso di PGPdisk
  - 21.7.3. Altre caratteristiche

## Capitolo XXII - La sicurezza informatica e la privacy

- 22.1 La sicurezza informatica
- 22.2. I requisiti di un sistema informatico sicuro
- 22.3. Le vulnerabilità della sicurezza dei sistemi informatici
- 22.4. La sicurezza del software
- 22.5. L'identificazione
- 22.6. I sistemi di autenticazione
- 22.7. La firma digitale

- 22.8. Il controllo degli accessi
- 22.9. La sicurezza della rete
- 22.10. L'importanza delle copie di backup
- 22.11. I firewall: la sicurezza in un filtro
- 22.12. Le installazioni predefinite dei sistemi operativi e delle applicazioni
- 22.13. Gli account senza password o con password "deboli"
- 22.14. I backup inesistenti o incompleti
- 22.15. Numero elevato di porte aperte
- 22.16. I pacchetti non vengono filtrati per determinarne il corretto indirizzo in ingresso e in uscita
- 22.17. Log inesistenti o non completi
- 22.18. Programmi CGI vulnerabili
- 22.19. Privacy e sicurezza dei dati
  - 22.19.1. Le novità del Codice sulla Privacy
  - 22.19.2. La sicurezza informatica (o Information Security)
  - 22.19.3. Le misure di sicurezza previste dal nuovo Codice
  - 22.19.4. Definizioni
  - 22.19.5. Misure di sicurezza
  - 22.19.6. Misure minime di sicurezza
  - 22.19.7. Trattamenti con strumenti elettronici
  - 22.19.8. Trattamento senza l'ausilio di strumenti elettronici
  - 22.19.9. Il Disciplinare Tecnico in materia di misure minime di sicurezza
  - 22.19.10. I trattamenti con strumenti elettronici
  - 22.19.11. Documento Programmatico sulla Sicurezza (DPSS)
  - 22.19.12. Trattamento dei dati sensibili o giudiziari
  - 22.19.13. Trattamenti senza l'ausilio di strumenti elettronici

## Capitolo XXIII - LA PROTEZIONE DAI VIRUS E DAI DIALERS

- 23.1. I virus informatici
  - 23.1.1. Gli attacchi tramite virus
  - 23.1.2. I virus in rete
  - 23.1.3. Altre tipologie di malicious codes: i "Cavalli di Troia" e i "Virus Macro"
  - 23.1.4. Le conseguenze dell'azione virale su hardware e software
- 23.2. La diffusione dei virus attraverso Internet e la posta elettronica
- 23.3. La prevenzione e i software antivirus
  - 23.3.1. Caratteristiche di base del software antivirus
- 23.4. I dialers
  - 23.4.1. La diffusione dei dialers
  - 23.4.2. Classificazione e tipologie dei dialers
  - 23.4.3. Come funzionano tecnicamente i dialers
  - 23.4.4. Le truffe attraverso dialers e 709