

INDICE

CAPITOLO I

LA GOVERNANCE MONDIALE DI INTERNET

1. Introduzione	1
2. Il tentativo di regolamentazione di Internet	4
3. Il problema delle fonti.....	7
4. I soggetti coinvolti	9
5. ICANN.....	9
6. ISOC	13
7. Una carta dei diritti per Internet?	16

CAPITOLO II

I NOMI A DOMINIO IN ITALIA

1. I <i>domain names</i>	21
2. La gestione dei nomi a dominio: il <i>Domain Name System</i> (DNS)	29
3. La registrazione del <i>domain name</i>	31
4. Dalla <i>Naming e Registration Authority</i> al “Registro”.....	34
5. Il Registro.....	37
6. Dalle regole di <i>Naming</i> al “Regolamento di assegnazione e gestione dei nomi a dominio –it”	39
7. Il nome a dominio come segno distintivo e il fenomeno del <i>domain grabbing</i>	42
8. La giurisprudenza sui nomi a dominio prima del codice della proprietà industriale del 2005.....	46
9. Il codice per la proprietà industriale del 2005	56
10. La giurisprudenza dei nomi a dominio dopo il codice sulla proprietà industriale..	60
11. I <i>new gTLD</i>	64

CAPITOLO III

**L'AGCOM – AUTORITÀ PER LE GARANZIE
NELLE COMUNICAZIONI**

1. Nascita ed evoluzione dell’Autorità per le garanzie nelle comunicazioni.....	69
2. L’Agcom e il diritto d’autore	74
3. Il ruolo dei Corecom	76
4. I Corecom e la definizione stragiudiziale delle controversie	78

CAPITOLO IV

**IL SISTEMA RADIOTELEVISIVO:
DALL’ANALOGICO AL DIGITALE**

1. Introduzione	83
2. Gli aspetti tecnici delle frequenze	85
3. L’evoluzione normativa	87
4. La liberalizzazione delle frequenze e il <i>beauty contest</i>	89
5. La TV digitale	91
6. I limiti alla concentrazione delle risorse	93
7. Il servizio pubblico radiotelevisivo.....	95

CAPITOLO V

**LA COMUNICAZIONE PUBBLICA ELETTRONICA
TRA PRIVACY E ACCESSO ALLA DOCUMENTAZIONE**

1. Introduzione	99
2. L’accesso alla documentazione amministrativa	102
3. La giurisprudenza sull’accesso	108
4. La comunicazione digitale nella P.A.....	112
5. L’Indice degli indirizzi delle pubbliche amministrazioni (IPA).....	114
6. La nozione di “documento amministrativo”	118

7. I certificatori e la riservatezza	121
8. Il fascicolo informatico e la riservatezza	122
9. Il Protocollo informatico e la riservatezza	124
10. La carta d'identità elettronica, la carta nazionale dei servizi, il passaporto elettronico	133
11. Le carte elettroniche della P.A. e la tutela dei dati contenuti ai fini della riservatezza	138
12. L'accessibilità in Rete dei dati	145
13. I rischi del trattamento dei dati nell' <i>e-gov</i>	150
14. Note critiche conclusive	154

CAPITOLO VI

ASPETTI TECNICI DELLA FIRMA DIGITALE: LA CRITTOGRAFIA

1. La crittografia	159
2. La crittoanalisi	162
3. Alcuni sistemi crittografici	163
4. La crittografia a chiave pubblica e il PGP	167
5. La funzione di <i>hash</i>	170
6. Il <i>time stamping</i>	173
7. Il <i>Key Escrow</i>	174
8. Cenni sulla chiave biometrica	175

CAPITOLO VII

LA FIRMA DIGITALE

1. L'evoluzione normativa della firma digitale prima del codice dell'amministrazione digitale (CAD)	177
2. Il documento informatico e la copia informatica nel CAD	180
3. Le firme elettroniche	184
4. Il valore giuridico e probatorio del documento informatico	188
5. Profili di responsabilità da uso abusivo o erroneo della firma digitale	194

- | | |
|--|-----|
| 6. Il momento di decorrenza degli effetti della revoca o sospensione del certificato... | 195 |
| 7. Tra le pieghe nascoste del “decreto del fare” 2013: le norme sulla digitalizzazione pubblica che incidono sulla vita dei cittadini..... | 196 |

CAPITOLO VIII

LA PEC

- | | |
|--|-----|
| 1. Evoluzione, natura e funzioni della PEC | 203 |
| 2. Il funzionamento della PEC | 206 |
| 3. Il ruolo dei Gestori | 210 |

CAPITOLO IX

IL RUOLO DEI CERTIFICATORI

- | | |
|--|-----|
| 1. L'attività di certificazione | 213 |
| 2. I certificatori qualificati | 217 |
| 3. I certificatori accreditati | 219 |
| 4. Gli obblighi dei certificatori | 221 |
| 5. Revoca e sospensione del certificato..... | 223 |
| 6. Profili di responsabilità dell'attività di certificazione | 226 |
| 7. Compiti e ruolo di DigitPA | 229 |

CAPITOLO X

COMPUTER CRIMES

- | | |
|---|-----|
| 1. Premessa | 235 |
| 2. Sistema informatico e telematico | 237 |
| 3. Abuso della qualità di operatore del sistema | 238 |
| 4. Esercizio arbitrario delle proprie ragioni con violenza sulle cose (Art. 392 c.p.).. | 240 |

5. Attentato a impianti di pubblica utilità (Art. 420 c.p.).....	241
6. Il falso documento informatico (Art. 491- <i>bis</i> c.p.).....	242
7. Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri (Art. 495- <i>bis</i> c.p.).....	248
8. Il reato di accesso abusivo ad un sistema informatico o telematico (Art. 615- <i>ter</i> c.p.)	249
9. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615- <i>quater</i> c.p.)	255
10. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615- <i>quinquies</i> c.p.).....	258
11. Tutela della corrispondenza informatica e telematica (Art. 616 c.p.).....	261
12. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617- <i>quater</i> c.p.).....	263
13. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617- <i>quinquies</i> c.p.)	265
14. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (Art. 617- <i>sexies</i> c.p.)	266
15. Il documento informatico segreto (Art. 621 c.p.)	267
16. Altre comunicazioni e conversazioni (Art. 623- <i>bis</i> c.p.)	268
17. Danneggiamento di informazioni, dati e programmi informatici (Art. 635- <i>bis</i> c.p.)	269
18. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635- <i>ter</i> c.p.)..	272
19. Danneggiamento di sistemi informatici o telematici (Art. 635- <i>quater</i> c.p.)....	274
20. Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635- <i>quinquies</i> c.p.).....	275
21. La frode informatica (Art. 640- <i>ter</i> c.p.).....	277
22. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640- <i>quinquies</i> c.p.).....	279
23. Le modifiche recenti: dalla convenzione di Budapest alla l. 48/2008	279

CAPITOLO XI

GLI ILLECITI IN RETE

1. Introduzione	283
2. I rischi delle “pagine eseguibili”	284
3. <i>Cookies</i>	285

4. <i>Spamming</i>	290
5. <i>Phishing</i>	296
6. <i>Sniffing</i>	301
7. <i>Wardriving e piggybacking</i>	303
8. <i>Data diddling</i>	309
9. <i>Trojan horse</i>	310
10. <i>Salami techniques</i>	311
11. <i>Spoofing</i>	311
12. <i>Superzapping</i>	312
13. <i>Trap dors</i>	313
14. <i>Logic bomb</i>	313
15. <i>Asynchronous attacks</i>	314
16. <i>Scavenging</i>	314
17. <i>Data leakage</i>	314
18. <i>Simulation and modeling</i>	314
19. <i>Denial of service (dos)</i>	315
20. Le responsabilità per gli illeciti in Internet.....	316
21. La responsabilità del provider.....	321

CAPITOLO XII

LA TUTELA DEL DIRITTO D'AUTORE IN RETE

1. Il diritto d'autore in Internet	335
2. L'Agcom e il ruolo di "censore" in Internet	336
3. Procedura ex art. 6 e ss. Allegato A alla delibera 398/11/CONS	340
4. Le fonti attributive di poteri all'AGCOM.....	344
5. La legge Hadopi in Francia.....	349
6. <i>Acta - Anti Counterfeiting Trade Agreement</i>	351

CAPITOLO XIII

DIGITAL FORENSICS

1. La definizione di <i>Digital Forensics</i>	357
---	-----

2. Ricerca e riconoscimento della prova informatica.....	358
3. Il modello di <i>O'Ciardhuain</i>	362
4. Raccolta e conservazione di prove informatiche	365
5. Il <i>Write-Blocker</i>	368
6. Analisi delle prove informatiche.....	371
7. La ricostruzione dei fatti attraverso le prove informatiche.....	373
8. L'utilizzabilità delle evidenze informatiche nel processo.....	374

CAPITOLO XIV

LA DISCIPLINA GENERALE DELLA TUTELA DEI DATI PERSONALI

1. Introduzione	383
2. I soggetti coinvolti nel trattamento	388
3. Modalità del trattamento dei dati.	390
4. L'interessato e i suoi diritti: conoscitivi e applicativi.	392

CAPITOLO XV

GLI ADEMPIMENTI DEL TITOLARE NEI CONFRONTI DEL GARANTE

1. Introduzione	401
2. La notificazione del trattamento.....	402
3. I tempi della notificazione.....	405
4. I trattamenti soggetti a notificazione.....	408
5. Il registro dei trattamenti.....	410
6. Le sanzioni.....	410
7. Le autorizzazioni generali.....	411
8. La verifica preliminare	413

CAPITOLO XVI

**GLI OBBLIGHI DEL TITOLARE NEI CONFRONTI
DELL'INTERESSATO**

1. Introduzione	417
2. L'informativa	419
3. Le funzioni dell'informativa	421
4. L'oggetto dell'informativa	422
5. I soggetti dell'informativa	424
6. La chiarezza dell'informativa	426
7. L'informativa abbreviata	428
8. L'esclusione dell'informativa per dati raccolti presso terzi	429
9. Indicazioni pratiche sull'adempimento	431
10. L'analisi storica del consenso	431
11. I soggetti tenuti a richiedere il consenso	433
12. La forma del consenso	434
13. Come effettuare la richiesta di consenso	437
14. Casi nei quali il trattamento può essere effettuato senza consenso	438

CAPITOLO XVII

**LE MISURE DI SICUREZZA MINIME E IDONEE E
PREVENTIVE**

1. Gli obblighi del titolare del trattamento e le misure di sicurezza	445
2. La sicurezza informatica nel Codice Privacy	449
3. Tipologie di minacce alla sicurezza	451
4. Misure "idonee e preventive" e misure "minime" di sicurezza	456
5. Le misure idonee e preventive	458
6. Le misure minime di sicurezza e l'allegato b)	466
7. L'abrogazione dell'obbligo di DPS (Documento Programmatico sulla Sicurezza) ..	479

CAPITOLO XVIII

**LE RESPONSABILITÀ E LE SANZIONI IN MATERIA
DI PRIVACY**

1. Il regime della responsabilità nella tutela dei dati personali.....	487
2. La responsabilità amministrativa e penale.....	494
3. Reati in materia di trattamento dei dati personali.....	499
4. Conclusioni.....	501
 <i>Bibliografia</i>	 503