

INDICE

CAPITOLO PRIMO IL FUNZIONAMENTO DI INTERNET

1. Cosa è Internet.....	1
2. ISOC.....	4
3. Il Domain Name System (DNS)	6
4. Dall'IP al nome a dominio	8
5. Il Top Level Domain e il Second Level Domain	10
6. I new gTLD	12
7. Da IANA a ICANN.....	15

CAPITOLO SECONDO LA REGOLAMENTAZIONE DI INTERNET

1. Le regole della Rete.....	21
2. Le tre possibili strade	23
3. La Net Neutrality.....	25
4. La censura in Interneto.....	27

CAPITOLO TERZO LA REGISTRAZIONE DI UN NOME A DOMINIO

1. La natura del nome a dominio.....	31
2. I requisiti per la registrazione del <i>domain name</i>	33
3. Il ruolo della RA e della NA.....	37
4. Il Registro.....	40
5. Dalle Regole di <i>naming</i> al “Regolamento di assegnazione e gestione dei nomi a dominio –it”	42

CAPITOLO QUARTO
LA TUTELA DEI SEGNI DISTINTIVI

1. Il cybersquatting e il domain grabbing.....	47
2. La giurisprudenza sui nomi a dominio prima del codice della proprietà industriale del 2005	52
3. Il codice della proprietà industriale del 2005	62
4. La giurisprudenza dei nomi a dominio dopo il Codice sulla proprietà industriale.....	66

CAPITOLO QUINTO
LA TUTELA DELLA PROPRIETÀ INTELLETTUALE

1. I diritti d'autore morali e patrimoniali	73
2. Le opere collettive e composte.....	77
3. La normativa europea: direttiva Barnier del 2014	78
4. La SIAE e gli altri enti di tutela del diritto d'autore	80
5. Soundreef	85
6. Le <i>Collecting Societies</i> a confronto	86
7. Il diritto d'autore in Rete.....	87
8. La protezione del software	89
9. L'AGCOM e il diritto d'autore	93
10. Le pronunce della Corte costituzionale sulle prerogative dell'AGCOM..	96

CAPITOLO SESTO
L'AGCOM E I CORECOM

1. Nascita ed evoluzione dell'Autorità per le Garanzie nelle Comunicazioni .	105
2. Il ruolo dei Co.re.com	109
3. I Co.re.com e la definizione stragiudiziale delle controversie	111

CAPITOLO SETTIMO
IL SISTEMA RADIOTELEVISIVO ITALIANO

1. Introduzione	117
2. Il <i>switch-off</i>	120
3. Gli aspetti tecnici delle frequenze	122
4. L'evoluzione normativa.....	124
5. Il TUSMAR e le modifiche del dicembre 2021	126
6. Il caso Vivendi vs. Mediaset	128
7. La liberalizzazione delle frequenze e il <i>beauty contest</i>	130

CAPITOLO OTTAVO
**LA DEMATERIALIZZAZIONE E LA DIGITALIZZAZIONE
DELLA PUBBLICA AMMINISTRAZIONE**

1. Introduzione	135
2. Il ruolo di AgID	139
3. Il fascicolo informatico	146
4. Il Protocollo informatico	148
5. I rischi del trattamento dei dati nell' <i>e-gov</i>	153

CAPITOLO NONO
**GLI STRUMENTI DI COMUNICAZIONE ELETTRONICA
DELLA P.A.**

1. Il sistema <i>SPID</i>	157
2. Le carte elettroniche del cittadino	161
2.1. La Carta d'Identità elettronica (CIE).....	163
2.2. La Carta Nazionale dei Servizi (CNS)	165
2.3. Il passaporto elettronico	167
3. Carte elettroniche e privacy	168

CAPITOLO DECIMO

LA PEC

1. Evoluzione, natura e funzioni della PEC	177
2. Il funzionamento della PEC	180
3. Il ruolo dei Gestori	184

CAPITOLO UNDICESIMO

**GLI ASPETTI TECNICI DELLA FIRMA DIGITALE:
LA CRITTOGRAFIA**

1. La crittografia	187
2. La crittoanalisi	190
3. Alcuni sistemi crittografici	191
4. La crittografia a chiave pubblica e il PGP	195
5. La funzione di <i>hash</i>	199
6. Il time stamping	201
7. Il <i>Key Escrow</i>	203
8. Cenni sulla chiave biometrica	203

CAPITOLO DODICESIMO

**IL DOCUMENTO ELETTRONICO
E LE FIRME ELETTRONICHE**

1. L'evoluzione normativa delle firme elettroniche	205
2. Il documento informatico e la copia informatica nel CAD	208
3. Le tipologie di firme elettroniche	212
4. Le definizioni di firme elettroniche	213
5. Il valore giuridico e probatorio del documento informatico e delle firme elettroniche	217
6. Profili di responsabilità da uso abusivo o erroneo della firma digitale .	219
7. Il momento di decorrenza degli effetti della revoca o sospensione del certificato	220

CAPITOLO TREDICESIMO
**LA DISCIPLINA GENERALE DELLA TUTELA DEI DATI
 PERSONALI**

1. Il GDPR.....	223
2. I concetti base.....	225
3. La privacy <i>by design</i> e <i>by default</i>	230
4. Il principio di <i>accountability</i>	232
5. I principi generali del trattamento.....	234
6. Le condizioni di liceità del trattamento.....	236

CAPITOLO QUATTORDICESIMO
GLI ADEMPIMENTI DEL TITOLARE

1. Le informazioni all'Interessato	243
2. Il Consenso.....	245
3. Il Registro delle attività di trattamento.....	249
4. La DPIA (Data Protection Impact Assessment).....	252
5. Il DPO (Data Protection Officer)	260
6. L'adozione di misure di sicurezza adeguate.....	269
7. Il Data Breach	272
8. Le tipologie di minacce alla sicurezza	276

CAPITOLO QUINDICESIMO
I DIRITTI DELL'INTERESSATO

1. Il diritto di accesso da parte dell'Interessato.....	281
2. L'accesso ai documenti amministrativi e l'accesso civico.....	285
3. Il diritto di rettifica	286
4. Il diritto alla cancellazione del dato (diritto all'oblio)	287
5. Il diritto di limitazione del dato.....	293
6. Il diritto alla portabilità del dato.....	294
7. Il diritto di opposizione	295
8. Il processo decisionale automatizzato e la profilazione	296
9. Le limitazioni all'esercizio dei diritti dell'interessato	301

CAPITOLO SEDICESIMO
**LA TUTELA GIUDIZIARIA E AMMINISTRATIVA
 DELLA PRIVACY**

1. Introduzione	305
2. Il reclamo al Garante	306
3. La segnalazione al Garante	310
4. Il ricorso davanti al giudice ordinario	311
5. Il risarcimento del danno.....	314
6. Le sanzioni	315
7. Le sanzioni amministrative	318
8. Le sanzioni penali	323

CAPITOLO DICIASSETTESIMO
GLI ASPETTI GENERALI DEI COMPUTER CRIMES

1. La L. 547 del 1993	333
2. Il sistema informatico e telematico	335
3. L'abuso della qualità di operatore del sistema	336

CAPITOLO DICIOTTESIMO
I COMPUTER CRIMES SU HARDWARE E SOFTWARE

1. L'esercizio arbitrario delle proprie ragioni con violenza sulle cose (Art. 392 c.p.).....	339
2. L'attentato a impianti di pubblica utilità (Art. 420 c.p.)	340
3. Il reato di accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)	341
4. La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater c.p.).....	347
5. La diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Articolo 615-quinquies c.p.)	351
6. Il danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.)	355

7. Il 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.).....	359
8. Il danneggiamento di sistemi informatici o telematici (Art. 635- <i>quater</i> c.p.)	361
9. Il danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635- <i>quinquies</i> c.p.)	363
10. La frode informatica (Art. 640- <i>ter</i> c.p.)	364
11. La frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640- <i>quinquies</i> c.p.).....	370

CAPITOLO DICIANNOVESIMO

I COMPUTER CRIMES SU DOCUMENTI

1. Il falso documento informatico (Art. 491- <i>bis</i> c.p.)	371
2. La 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.)...	378
3. Il documento informatico segreto (Art. 621 c.p.).....	379

CAPITOLO VENTESIMO

I COMPUTER CRIMES SU COMUNICAZIONI E CORRISPONDENZA

1. La tutela della corrispondenza informatica e telematica (Art. 616 c.p.)..	381
2. L'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617- <i>quater</i> c.p.)	382
3. L'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617- <i>quinquies</i> c.p.)	386
4. La falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (Art. 617- <i>sexies</i> c.p.).....	387
5. Le altre comunicazioni e conversazioni (Art. 623- <i>bis</i> c.p.).....	388

CAPITOLO VENTUNESIMO
**LA RESPONSABILITÀ DELL'INTERNET
 SERVICE PROVIDER**

1. Le responsabilità per gli illeciti in Internet	391
2. La disciplina del <i>provider</i>	395
3. La prima giurisprudenza sulla responsabilità del <i>provider</i>	398
4. L'evoluzione del concetto di <i>hosting provider</i> “attivo” e “passivo”	407
5. La responsabilità dell' <i>hosting provider</i> “attivo”	413
6. La neutralità dell'ISP	415
7. Gli aspetti tecnici e il “ <i>fingerprinting</i> ”	417
8. Il regime di responsabilità del provider attivo	419
9. Il meccanismo della segnalazione al provider e l'indicazione specifica degli URL.....	422

CAPITOLO VENTIDUESIMO
LA DIGITAL FORENSICS

1. La definizione di <i>Digital Forensics</i>	427
2. La Convenzione di Budapest e la L. 48/2008	428
3. Le modifiche del secondo protocollo addizionale del 2022.....	431
4. La ricerca ed il riconoscimento della prova informatica.....	435
5. Il modello <i>O'Ciardhuain</i>	438
6. La raccolta e la conservazione di prove informatiche.....	441
7. Il write-blocker.....	444
8. L'analisi delle prove informatiche.....	448
9. La ricostruzione dei fatti attraverso le prove informatiche	449
10. La fruibilità delle evidenze informatiche nel processo	451
 BIBLIOGRAFIA.....	 459