# SOMMARIO

## DEL VOLUME I


**Prefazione** di Pietro GRASSO XXI
**Prefazione** di Domenico VULPIANI XXIII
**Introduzione** XXIX

CAPITOLO 1
**NOZIONI ED ELEMENTI TECNICI DI PRINCIPIO**
a cura di Gerardo COSTABILE

1. *Computer forensics & digital investigation:* definizioni e punti di attenzione 3
2. *Digital evidence*: cenni tecnici di base 6
2.1 Classificazione delle "evidenze digitali" 7
2.1.1 Dati e *log* sui sistemi coinvolti: cenni 8
2.1.2 *Log* e informazioni degli elementi infrastrutturali della rete o di sistemi di supporto: cenni 9
3. Le *best practices* sulla *computer forensics* 10
4. Le fasi del processo di *computer forensics* 18
5. *Computer forensics*: le classificazioni tipiche 18
6. La cd. *preview* 20
7. Le 10 regole d'oro della *computer forensics* e i 7 comportamenti da evitare 21

CAPITOLO 2
**LA RICEZIONE DELLA *NOTITIA CRIMINIS*:
I PRIMI PASSI VERSO UNA CORRETTA
INDIVIDUAZIONE ED ACQUISIZIONE DEGLI ELEMENTI
DI PROVA DI NATURA INFORMATICA**

a cura di Francesco CAJANI

1. Nozione giuridica di "*digital evidence*" (prova elettronica o digitale) 27
2. Cenni generali sugli accertamenti informatici nelle investigazioni penali e classificazione "operativa" dei reati informatici genericamente intesi 30
3. L'acquisizione della *notitia criminis* 34
4. L'acquisizione della denuncia e della denuncia-querela ad opera della Polizia Giudiziaria 35
4.1 La "ragionevole tempestività" nella trasmissione della comunicazione di notizia di reato e la necessità di individuare dei protocolli di Polizia Giudiziaria volti alla corretta acquisizione della denuncia querela 37
4.1.1 segue: Informazioni che la persona offesa dovrebbe fornire in sede di denuncia querela 41
4.2 Gli atti di indagine che si possono compiere in mancanza della condizione di procedibilità 43
4.3 L'assenza della condizione di procedibilità: casi pratici e conseguenze 43
5. Le ipotesi di arresto in flagranza e di fermo di indiziato di reato, in relazione ai reati informatici 53
5.1 segue: L'utilizzo indebito di carte di credito e altri strumenti di pagamento; il loro illecito possesso e/o falsificazione 56
5.2 segue: Il *phishing* e le ipotesi di *cyberriciclaggio* 59
6. Gli allegati alla denuncia querela o alla comunicazione di notizia di reato: in particolare l'acquisizione di una pagina web o di un intero sito; la produzione di una pagina web su supporto cartaceo e la sua valenza probatoria 78
6.1 segue: Gli aspetti tecnici per una corretta acquisizione processuale di informazioni presenti sulla Rete 80
6.2 segue: Esempio di acquisizione di un sito web 82

7. Furto di identità sul Web e primi accertamenti di Polizia Giudiziaria volti alla ricerca delle fonti di prova (cenni) 85
7.1 segue: I primi accertamenti di Polizia Giudiziaria in relazione alle ipotesi di furto di identità su piattaforme di commercio elettronico (in particolare *eBay*) 92
7.2 segue: L'analisi della movimentazione dei conti correnti relativi alle cd. banche *online* 96
7.3 segue: Gli altri strumenti di pagamento che possono venire utilizzati per conseguire l'illecito profitto. In particolare il vaglia *online* 96
7.4 segue: La pericolosità del truffatore seriale e la possibilità di applicazione di una misura di prevenzione. Il caso M. 99
8. Gli accertamenti sulle transazioni in frode a mezzo di istituti di *money transfer* 110
8.1 La transazione "*To Send Money*" 111
8.2 La richiesta dati agli operatori *money transfer* 116
9. L'ambito operativo degli accertamenti di Polizia Giudiziaria relativi alle falsificazione delle carte di credito 116
10. Le (altre) indagini scientifiche in ausilio alla *computer forensics* 126
11. Due parole sui supporti di memorizzazione utilizzati 133

CAPITOLO 3
**I *FILE* DI *LOG***
**E LA CONSERVAZIONE DEI DATI AZIENDALI:**
**ASPETTI INVESTIGATIVI E TECNICI DI BASE**
a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa: definizione e aspetti giuridici 137
2. Sicurezza dei *log* 138
3. Individuazione dei sistemi e primi passi 139
4. Amministratori di sistema 140
5. Tempi di conservazione dei *log* 141
6. Servizi di comunicazione elettronica e *log files* 142
7. Categorie di dati da conservare 143
8. Vincoli temporali di conservazione dei dati 146
9. Misure di sicurezza 148
9.1 Autenticazione 148

9.2 Autorizzazione 149
9.3 Conservazione e protezione dei dati 150
9.4 Tracciamento delle attività 151

CAPITOLO 4
**ASPETTI GIURIDICI COMUNI DELLE INDAGINI INFORMATICHE**

a cura di Francesco CAJANI (parte I, II, IV sez. II, V, VI sez. II, X, XI) e di Stefano ATERNO (parte III, IV sez. I, VI sez. I, VII, VIII, IX)

**PARTE I - GIURISDIZIONE**
1. I problemi di giurisdizione nell'attività di individuazione e raccolta delle evidenze digitali 157
1.1 2001/2008 Odissea nel *Cyberspazio* 159
1.2 Verso un nuovo concetto di cooperazione internazionale 163
1.3 Gli organismi di coordinamento giudiziario ed investigativo a livello europeo 168
1.3.1 Eurojust 169
1.3.2 Europol 171
1.3.3 Interpol 172
1.3.4 OLAF 172
1.4 Gli organismi di cooperazione internazionale 173
1.4.1 Il Consiglio d'Europa 173
1.4.2 I punti di contatto nazionali (Rete 24/7) 176
1.4.3 Ipotesi di collaborazione tra le Forze di Polizia ed il cd. settore privato: le *task force* in materia di *computer crimes* 178
1.5 Problemi di giurisdizione in materia di siti o pagine web allocate su *server* esteri 181
1.6 Cooperazione e coordinamento investigativo nelle ipotesi di reati transnazionali: il sequestro (anche per equivalente) di beni all'estero 182

**PARTE II - COMPETENZA TERRITORIALE**
1. La competenza territoriale in relazione alle indagini informatiche 193
1.1 I differenti criteri volti ad individuare il *locus commissi delicti* nelle truffe *online ex* art. 640 c.p. e l'opportunità di valorizzare soluzioni idonee a far emergere la serialità dei fatti reato 194

1.1.1. L'impostazione di recente adottata dalla Procura Generale presso la Corte di Cassazione laddove i profitti della truffa *online* vengano indirizzati su un conto corrente (e non già su una carta ricaricabile) 200
1.2 L'individuazione del "domicilio informatico" come criterio idoneo a radicare la competenza territoriale nelle ipotesi *ex* art. 615-*ter* c.p. (accesso abusivo) 202
1.3 Il *locus commissi delicti* nei casi di diffamazione *online ex* art. 595 comma 3 c.p 206
1.4 Il *locus commissi delicti* nei casi di *phishing* e di *cyberriciclaggio* 226
1.5 Il *locus commissi delicti* in relazione ad altri reati commessi *online* (cenni) 234

**PARTE III - LA NUOVA COMPETENZA FUNZIONALE *EX* ART. 11 LEGGE 48/2008**
1. I lavori parlamentari della legge 18 marzo 2008, n. 48: brevi cenni 238
2. La previsione di una competenza territoriale "distrettuale" *ex* art. 11 legge 48/2008 per i reati informatici 244
3. Alcune osservazioni critiche sulla previsione di una competenza territoriale distrettuale per i *computer crimes* 244

**PARTE IV - LA DISCIPLINA IN TEMA DI CONSERVAZIONE DEI DATI (*DATA RETENTION*)**

SEZIONE I - ANALISI DELLE NORME APPLICABILI
1. Le fonti nazionali e le fonti europee in materia di *data retention* 249
1.1 Le Direttive 95/46/CE e 97/66/CE 249
1.2 La Direttiva 2002/58/CE 251
1.3 Il c.d. decreto Pisanu (d.l. n. 144/2005, convertito in legge n. 155/2005) 253
1.4 La Direttiva 2006/24/CE 254
2. Il provvedimento del Garante per la protezione dei dati personali del gennaio 2008 in materia di *data retention* 266
2.1 Le tipologie dei dati da conservare: dati relativi al traffico, anagrafiche e "dati di traffico" 268
3. Le recenti modifiche della normativa sulla *data retention* in seguito all'attuazione della Direttiva 2006/24/CE con il d.lgs. 109 del 2008: come cambia l'art. 132 del Codice privacy 272

3.1 I "dati relativi al traffico" e le altre definizioni normative 273
3.2 Le vicende temporali della *data retention* 277
3.2.1 Le proroghe del d.l. 2 ottobre 2008 n.151 281
3.3 I periodi temporali di conservazione *ex* art. 132 Codice privacy e l'art. 254-*bis* c.p.p. 282
3.3.1 I poteri, le modalità e i tempi delle parti nelle richieste dei dati di traffico ai gestori 285
3.3.2 Conclusioni circa i rapporti tra art. 132 Codice privacy e l'art. 254-*bis* c.p.p 293
3.4 Le chiamate senza risposta 296
3.5 Le abrogazioni stabilite dal d.lgs. n. 109 del 2008 298
3.6 Indirizzo di *Internet protocol*: cosa conservare e cosa cancellare? 300
3.7 Il monitoraggio delle attività di acquisizione e di trattamento dei dati 305
3.8 Le sanzioni (art. 162-*bis* Codice Privacy e art. 5 comma 2 d.lgs. 109/2008) 306
4. Il *freezing* dei dati telematici previsto dal comma 4-*ter* e ss dell'art. 132 Codice privacy 308
5. Una storia non ancora finita: libero Wi-fi in libero Stato… 312

SEZIONE II - INVESTIGAZIONE VS. PRIVACY: IL BILANCIAMENTO DEGLI OPPOSTI INTERESSI
1. Garanti UE vs. Direttiva UE 320
2. Il paradosso della *privacy*: il caso del cd. "blog anti-premier" 323

**PARTE V - LA FASE DI ACQUISIZIONE DEGLI ELEMENTI DI PROVA DIGITALE: ATTIVITÀ IRRIPETIBILE O RIPETIBILE?**
1. Gli accertamenti urgenti di cui all'art. 354 c.p.p. 367
1.1 Ripetibilità o irripetibilità tecnica dell'attività di *computer forensics* 372
2. Gli accertamenti tecnici *ex* artt. 359 e 360 c.p.p. 374
3. Comportamenti "maldestri" della Polizia Giudiziaria sulla *scena criminis* informatica: il caso Garlasco 380
4. L'opportunità di disporre una analisi forense di un reperto informatico *ex* art. 360 c.p.p. 385
5. Gli accertamenti e i rilievi delegati dal Pubblico Ministero alla Polizia Giudiziaria 387

**PARTE VI - PERQUISIZIONE ED ISPEZIONE**

SEZIONE I – L'ANALISI DELLE NORME DEL C.P.P.
1. Art. 247 c.p.p. e art. 352 c.p.p.: differenze applicative dei due strumenti investigativi 393
2. Il significato tecnico – giuridico di perquisizione su un sistema informatico o telematico e su supporto informatico 398
3. Duplicazione su supporti. Conservazione ed inalterabilità dei dati originali. Garanzia della conformità della copia all'originale e sua immodificabilità 404
4. L'ispezione di un sistema informatico alla luce della novella del 2008: cosa cambia rispetto al passato? 408

SEZIONE II - LE "NUOVE FRONTIERE" DELL'INVESTIGAZIONE DIGITALE ALLA LUCE DELLA LEGGE 48/2008, OVVERO: QUELLO CHE LE NORME NON DICONO
1. L' ispezione di un *client* ubicato in Italia (ma interconnesso ad un server allocato all'estero) e la relativa acquisizione degli elementi di prova digitale ivi complessivamente presenti 413
2. L'accesso "da remoto" ad una casella di posta elettronica e la relativa acquisizione degli elementi di prova digitale ivi complessivamente presenti 417
2.1 La c.d. perquisizione *online*, questa sconosciuta 418
2.2 La consapevole rivelazione delle credenziali di accesso di una casella di posta elettronica 421
2.2.1 *Case study*: accesso ad una casella di posta elettronica *@yahoo.com* (le cui credenziali di accesso erano state rivelate dall'indagato, durante l'interrogatorio del Pubblico Ministero alla presenza del difensore) 422
2.3 La conoscenza delle credenziali di accesso in capo alla Polizia Giudiziaria senza che l'utilizzatore ne abbia consapevolezza 434
3. L' accesso "da remoto" ai messaggi in bozze di una casella di posta elettronica utilizzata come "bacheca" e la relativa acquisizione degli elementi di prova digitale ivi complessivamente presenti 438
4. *Case study*: analisi forense di computer portatili con cifratura dell'intero *hard disk* 439

**PARTE VII - RICHIESTA DI CONSEGNA E SEQUESTRO DEI DATI DIGITALI**
1. La richiesta di consegna di dati, informazioni e programmi informatici ai sensi dell'art. 248 c.p.p. 460
2. Il sequestro di sistemi informatici e telematici e di supporti digitali 462
3. Le previsioni e le modifiche della legge 18 marzo 2008, n. 48: casi particolari 480
3.1 Il sequestro di corrispondenza anche se inoltrata per via telematica *ex* art. 254 c.p.p. (cenni e rinvio) 481
3.2 Il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni *ex* art. 254-*bis* c.p.p. 487
4. La custodia delle cose sequestrate *ex* art. 259 c.p.p. 490
5. L'apposizione dei sigilli e le cautele dell'art. 260 c.p.p. alle copie c.d. digitali 492

**PARTE VIII - IL CONSULENTE TECNICO, IL PERITO E LO SVOLGIMENTO DELLE ATTIVITÀ PREVISTE DAL CODICE DI PROCEDURA PENALE. RESPONSABILITÀ**
1. Le fonti normative 496
2. La consulenza tecnica 497
2.1 Ambito e attività 497
2.2 La nomina del consulente tecnico; il conferimento dell'incarico 500
2.3 Consulenza tecnica fuori dai casi di perizia 507
2.4 Incompatibilità e astensione del consulente 508
2.5 Il quesito tipo al consulente 509
2.5.1 Due quesiti in materia di indagini informatiche 511
3. La perizia: Natura e ambito di operatività 513
4. Ammissibilità della perizia e discrezionalità del Giudice 516
4.1 La valutazione dei risultati da parte dell'organo giudicante 524
5. La nomina del perito 531
5.1 La scelta del perito 531
5.2 Incapacità e incompatibilità 536
5.3 Astensione e ricusazione 538
5.4 Obblighi del perito 540
5.5 La liquidazione del compenso al perito (art. 232 c.p.p.) 541

6. I provvedimenti del Giudice che dispone la perizia 543
6.1 Attività del Giudice 543
6.2 Ordinanza (contenuto) 546
6.3 Conferimento dell'incarico e formulazione dei quesiti 547
7. L'attività del perito e la relazione 549
7.1 Attività del perito 549
7.2 La relazione peritale 553
7.3 Le comunicazioni alle altre parti 558
8. L'incidente probatorio 560
9. Le responsabilità penali del perito e del consulente tecnico 564
9.1 Falsa perizia o interpretazione (art. 373 c.p.) 564
9.2 Frode processuale (art. 374 c.p.) 567
9.3 Intralcio alla giustizia (art. 377 c.p.) 573

**PARTE IX - LE INDAGINI DIFENSIVE E L'ALIBI INFORMATICO**
1. L'indagine difensiva in generale e il ruolo del Difensore 576
2. Le diverse sottospecie di indagini difensive 581
2.1 Le indagini preventive 581
2.2 Le indagini suppletive 583
2.3 Le indagini integrative 583
3. I poteri e limiti del Difensore e del suo consulente tecnico 584
3.1 L'accesso ai luoghi 587
3.2 L'accertamento tecnico ripetibile e irripetibile 589
3.3 L'esame delle cose sequestrate 590
4. La richiesta di documenti alla pubblica amministrazione e ai privati; il diniego dei documenti. La particolare richiesta ai gestori telefonici dei tabulati di traffico telefonico e telematico 591
5. L'alibi informatico 595

**PARTE X - IL VAGLIO DIBATTIMENTALE DELLA *DIGITAL EVIDENCE*: LA RIPARTIZIONE DELL'ONERE PROBATORIO TRA ACCUSA E DIFESA E LE CONSEGUENZE IN PUNTO DI NON CORRETTA ACQUISIZIONE DEGLI ELEMENTI DI PROVA DIGITALE**
1. Le questioni relative alla "attendibilità" dei *log files* 601
2. Il valore probatorio dell'immagine digitale: originale o copia? 607

3. Il dibattito dottrinale sugli effetti dell'assenza o della non corretta adozione delle misure volte a salvaguardia delle genuinità della evidenza digitale 609
3.1 La prima sentenza della Suprema Corte dopo l'introduzione della legge 48/2008 617
3.2 I lavori parlamentari 618
3.3 Le critiche alla tesi delle prove c.d. incostituzionali 620
3.4 Mondo reale e realtà virtuale 624
3.5 Il Giudice, la Prova e la Scienza 626
3.6 La prova pre-costituita 627
3.7 L'importanza dei protocolli operativi in materia di *digital evidence* 632
4. Il "caso Garlasco" e la soluzione giuridica adottata dal Giudice di primo grado in relazione agli effetti della "scorretta azione degli organi inquirenti sul computer" dell'indagato 634
5. La ripartizione dell'onere probatorio tra Accusa e Difesa 641

**PARTE XI - LA CONFISCA DEI BENI INFORMATICI**
1. La destinazione dei beni informatici sequestrati e confiscati: lo stato attuale della normativa e una proposta di legge (ddl. n. 2271, approvato dal Senato della Repubblica, e successivo ddl. n. 4166 presentato alla Camera ed in corso di discussione) per una maggiore azione di contrasto al *cybercrime* 646