



L'estratto che stai visualizzando  
è tratto da un volume pubblicato su  
ShopWKI - La libreria del professionista

[VAI ALLA SCHEDA PRODOTTO](#)

## SOMMARIO

<b>Presentazione</b> .....	XXXIII
<i>di Michele Papa</i>	

### Parte I

#### **Diritto penale sostanziale: Questioni e prospettive di fondo**

##### **Capitolo I – Profili tecnico-informatici e filosofici**

*di Ugo Pagallo*

1. Prologo.....	3
2. Lo stato di diritto .....	4
3. La tecnologia .....	7
4. Codici informatici, codici giuridici .....	12
5. La ri-ontologizzazione del diritto .....	17
6. Ritorno allo stato di diritto (conclusioni) .....	21
7. Apparato bibliografico.....	29

##### **Capitolo II – Diritto penale e tecnologie informatiche: una visione d’insieme**

*di Lorenzo Picotti*

1. La rivoluzione tecnologica ed il suo impatto sui rapporti sociali e giuridici.....	35
1.1. Mutamenti indotti dallo sviluppo tecnologico e “rivoluzione” cibernetica.....	36
1.2. Dalla Rete al <i>Cyberspace</i> .....	38
1.3. Reciprocità di condizionamento fra realtà cibernetica e diritto....	40
2. Rilevanza giuridico-penale dell’ <i>automazione</i> quale “sostituzione” (parziale) dell’attività e del controllo dell’uomo .....	43
3. Il passaggio dai <i>Computer crime</i> ai <i>Cybercrime</i> .....	46
4. Il <i>web</i> interattivo ed il doppio ruolo degli utenti quali possibili autori e vittime di reati cibernetici .....	55
5. Tecniche di tipizzazione dei reati informatici e cibernetici e relative partizioni classificatorie.....	59

5.1.	Nuove condotte, estensioni “analogiche”, nuovi oggetti materiali .....	59
5.1.1.	Nuove condotte e nuovi “fatti” di reato: le fattispecie paradigmatiche della frode informatica e dell’accesso abusivo .....	60
5.1.2.	Estensioni per “analogia” legislativa di fattispecie preesistenti a nuovi oggetti “materiali” e relative modalità di condotta.....	66
5.2.	Collocazione sistematica e beni giuridici protetti .....	71
5.3.	Partizioni dei reati informatici e cibernetici .....	75
5.3.1.	I Reati informatici in senso stretto.....	75
5.3.2.	I Reati informatici in senso ampio.....	76
5.3.3.	Reati cibernetici .....	77
6.	Obblighi di tutela penale degli <i>Internet Service Providers</i> e sviluppi della giurisprudenza europea.....	81
6.1.	Giurisprudenza CEDU.....	83
6.2.	Giurisprudenza CGUE.....	85
7.	Osservazioni conclusive: verso un mutamento di nozioni basilari quale quella di consumazione del reato nel <i>Cyberspace</i> ? .....	89

**Capitolo III – Cyber-criminality: le fonti internazionali ed europee**

*di Roberto Flor*

Premessa metodologica

1.	Le fonti internazionali ed il sistema interno: dagli “albori” del diritto penale dell’informatica alla Convenzione <i>Cybercrime</i> .....	98
2.	Le fonti UE ante Lisbona.....	107
3.	Le fonti UE post Lisbona.....	115
4.	Uno sguardo necessario al ruolo “propulsore” della Corte di Giustizia.....	126
4.1.	Il caso “Google/Spain” .....	128
4.2.	La sentenza della Corte di Giustizia sulla c.d. <i>data retention</i> : un importante passo per il rafforzamento del diritto alla riservatezza. Ma con quali effetti per il sistema di giustizia penale? .....	131
5.	<i>Last but not least</i> : il nuovo regolamento europeo in materia di protezione dei dati personali (rinvio), la Dir. 2016/680/UE e la proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.....	134

## Capitolo IV – La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative

di Roberto Flor

1. Introduzione.....	142
2. Prima premessa di ordine generale: il diritto penale italiano.....	144
3. Seconda premessa di ordine generale: la Convenzione <i>Cybercrime</i> ....	148
4. Terza premessa di ordine generale: le fonti europee.....	148
5. Il <i>locus commissi delicti</i> nel <i>cyberspace</i> .....	150
5.1. Il caso della diffamazione.....	155
5.2. Il caso delle truffe <i>online</i> .....	161
5.2.1. (Segue) Le ipotesi di truffa comune realizzata attraverso l'utilizzo di strumenti tecnologici o la rete.....	162
5.2.2. (Segue) Le ipotesi di frode informatica aggravata dal furto o dall'indebito utilizzo dell'identità digitale in danno di uno o più soggetti.....	167
5.3. Il caso dell'accesso abusivo a sistemi informatici o telematici....	175
6. Considerazioni di sintesi.....	191

## Capitolo V – La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001

di Désirée Fondaroli

1. Premessa.....	193
2. La responsabilità degli enti ex D.Lgs. n. 231/2001.....	194
3. I reati informatici, presupposto della responsabilità degli enti.....	201
4. Privacy e D.Lgs. n. 231/2001.....	206

### Parte II

#### Diritto penale sostanziale: Tematiche di carattere specifico

### Capitolo I – Delitti con finalità di terrorismo con specifiche aggravanti “tecnologiche”

di Stefano Dambrosio con la collaborazione, in fase di ricerca, dell'Avv. Vittorio Cuoco

1. Inquadramento.....	211
2. Addestramento ad attività con finalità di terrorismo anche internazionale.....	212
3. Istigazione e apologia di terrorismo.....	213

**Capitolo II – Il cyberterrorismo di matrice religiosa**

*di Stefano Dambroso con la collaborazione, in fase di ricerca, della Dott.ssa Ludovica Purini e dell’Avv. Guido Di Donato*

1. Inquadramento .....	217
2. Cybersecurity e cyberterrorismo .....	218
3. Le direttrici della riforma EUROPEA per il futuro della cybersecurity .....	222
4. Il panorama normativo nazionale e l’architettura istituzionale cyber (D.P.C.M. 17.2.2017).....	224

**Capitolo III – L’istigazione a delinquere via web**

*di Michele Boggiani*

1. Introduzione.....	227
2. Bene giuridico protetto: l’ordine pubblico e i beni finali dei delitti oggetto di istigazione e apologia .....	228
3. Il soggetto attivo .....	229
4. Elemento oggettivo: in particolare, la compatibilità delle condotte istigatrici e apologetiche con l’art. 21 Cost. ....	229
5. (Segue) La pubblicità della condotta .....	231
6. (Segue) I destinatari della condotta .....	232
7. (Segue) La circostanza aggravante di cui al comma 3 e 4 – commissione del fatto attraverso strumenti informatici o telematici.....	232
8. Elemento soggettivo .....	233
9. La pena prevista .....	233
10. Rapporti con altre figure di reato.....	234

**Capitolo IV – L’Istigazione a pratiche di pedofilia e di pedopornografia**

*di Michele Boggiani*

1. Introduzione: l’art. 414- <i>bis</i> in rapporto alla Convenzione di Lanzarote del 2007 .....	237
2. Bene giuridico protetto: l’ordine pubblico e i beni finali dei delitti oggetto di istigazione e apologia .....	239
3. Il soggetto attivo .....	241
4. Il soggetto passivo .....	241
5. Elemento oggettivo: in particolare, la compatibilità delle condotte istigatrici e apologetiche con l’art. 21 Cost. ....	241

6. (Segue) La pubblicità della condotta .....	245
7. (Segue) I destinatari della condotta .....	245
8. Elemento soggettivo .....	246
9. La pena prevista.....	247
10. Rapporti con altre figure di reato.....	247

## **Capitolo V – L’associazione per delinquere “informatica”**

*di Nicolò Bussolati*

1. I sodalizi criminali e la rete.....	249
2. L’associazione per delinquere informatica nel quadro normativo esistente .....	252
3. Le particolarità morfologiche delle comunità virtuali.....	255
4. Le associazioni per delinquere finalizzate allo scambio di materiale pedopornografico.....	257
5. Le associazioni per delinquere finalizzate agli attacchi informatici ....	262

## **Capitolo VI – Le falsità informatiche**

*di Giandomenico Salcuni*

1. Premessa .....	273
2. Questioni intertemporali.....	275
3. Soggetto attivo ed elemento soggettivo .....	276
4. La condotta .....	277
5. Oggetto materiale .....	280
6. Forme di manifestazione del reato.....	283

## **Capitolo VII – La tutela penale delle carte di pagamento**

*di Andrea Galante*

1. L’origine e lo scopo della tutela penale delle carte di pagamento.....	285
2. L’evoluzione della tutela a seguito dello sviluppo dei sistemi di pagamento.....	287
3. L’oggetto materiale della tutela: carte di credito, di pagamento o documenti analoghi.....	289
4. L’indebito utilizzo di carte di pagamento .....	293
5. La falsificazione o alterazione di carte di pagamento .....	300
6. Il possesso, la cessione o l’acquisizione di carte di pagamento di provenienza illecita.....	302

**Capitolo VIII – La sostituzione di persona mediante furto di identità digitale**

*di Marisa Marraffino*

1. Premesse .....	307
2. Il bene giuridico protetto dalla norma e gli elementi costitutivi del reato .....	311
3. L'elemento soggettivo.....	316
4. Il phishing e le nuove falsificazioni digitali .....	316
5. False identità virtuali e Reg. UE 2016/679.....	319
6. Acquisizione delle prime evidenze digitali e problemi esecutivi.....	321
7. Profili amministrativi: l'azione davanti al Garante per la protezione dei dati personali.....	323
8. Le possibili responsabilità del fornitore di servizi legate al furto di identità .....	325
9. Conclusioni.....	329

**Capitolo IX – La diffamazione via web nell'epoca dei *social network***

*di Francesco Pio Lasalvia*

1. Premessa .....	331
2. La diffamazione come reato tradizionale commesso via <i>internet</i> .....	334
3. La qualificazione giuridica: il <i>web</i> è sempre “mezzo di pubblicità”? ....	341
4. La (ir)responsabilità delle figure diverse dall'autore della diffamazione .....	350
5. <i>Internet</i> spazio senza confini. Problemi di individuazione del <i>locus commissi delicti</i> .....	360
6. Tra libertà <i>del web</i> e sicurezza <i>sul web</i> . Brevi spunti di riflessione <i>de iure condendo</i> .....	366

**Capitolo X – La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p.**

*di Stefano Delsignore*

1. Premessa .....	374
2. Le ragioni dell'introduzione del delitto di pornografia minorile.....	376
3. Il recepimento della “Convenzione di Lanzarote” con la L. 1.10.2012, n. 172 .....	379
4. Collocazione sistematica e bene giuridico tutelato .....	381
4.1. Le non condivisibili tesi dottrinali che individuano il bene giuridico nella libertà di autodeterminazione sessuale e nella dignità umana.....	390

5. La natura di reati di pericolo astratto dei delitti di cui all'art. 600-ter.....	395
6. Le fattispecie previste dall'art. 600-ter c.p.....	402
7. Soggetto attivo .....	403
8. Soggetto passivo .....	404
9. La nozione di pornografia minorile.....	407
9.1. Le elaborazioni dottrinali e giurisprudenziali che hanno preceduto la nuova definizione normativa.....	407
9.2. La nuova definizione normativa di pornografia minorile introdotta nel 2012.....	412
9.3. La diretta rilevanza di alcune ipotesi di pornografia minorile parzialmente virtuale nell'ambito delle fattispecie previste dall'art. 600-ter. I rapporti con l'art. 600- <i>quater</i> .1 .....	418
10. I delitti previsti dall'art. 600-ter, comma 1: realizzazione di esibizioni o spettacoli pornografici; produzione di materiale pornografico minorile; induzione o reclutamento dei minori a partecipare ad esibizioni o spettacoli pornografici; percezione di altro profitto dai suddetti spettacoli .....	423
10.1. Il delitto di realizzazione di esibizioni o spettacoli pornografici utilizzando minori.....	430
10.2. Il delitto di produzione di materiale pornografico minorile.....	434
10.3. Il delitto di induzione o reclutamento dei minori a partecipare ad esibizioni o spettacoli pornografici.....	436
10.4. Il delitto di percezione di altro profitto dai suddetti spettacoli.....	438
10.5. Elemento soggettivo .....	439
10.6. Individuazione dei momenti consumativi e configurabilità del tentativo.....	440
11. Il delitto previsto dall'art. 600-ter, comma 2: commercio del materiale pedo-pornografico.....	442
11.1. Elemento oggettivo.....	442
11.2. Elemento soggettivo .....	444
11.3. Individuazione del momento consumativo e configurabilità del tentativo.....	444
12. I delitti previsti dall'art. 600-ter, comma 3: distribuzione, divulgazione, diffusione e pubblicizzazione di materiale pedopornografico; distribuzione e divulgazione di notizie o informazioni finalizzate all'adescamento e allo sfruttamento sessuale dei minori .....	445
12.1. Elemento oggettivo: le condotte tipiche .....	446
12.2. I mezzi di commissione. Il problema delle <i>chat-line</i> e degli <i>Internet Service Providers</i> .....	448

12.3. L'oggetto materiale .....	451
12.4. Elemento soggettivo .....	454
12.5. Individuazione del momento consumativo e configurabilità del tentativo.....	457
13. Il delitto dell'art. 600-ter, comma 4: offerta e cessione di materiale pornografico.....	458
13.1. Elemento oggettivo. Le condotte.....	458
13.2. L'oggetto materiale: «materiale pornografico di cui al primo comma».....	460
13.3. Elemento soggettivo .....	461
13.4. Individuazione del momento consumativo e configurabilità del tentativo.....	462
14. Il “nuovo” delitto previsto dal comma 6 dell'art. 600-ter: assistere ad esibizioni o spettacoli pornografici minorili.....	462
14.1. Elemento soggettivo .....	463
14.2. Individuazione del momento consumativo e configurabilità del tentativo.....	464
15. L'aggravante dell'ingente quantità prevista dal comma 5, le aggravanti di cui all'art. 602-ter c.p., l'attenuante prevista dall'art. 600-septies.1 c.p. e i profili sanzionatori .....	464
16. La confisca obbligatoria prevista dall'art. 600-septies c.p. e l'applicabilità ai delitti di produzione e di commercio di materiale pornografico della confisca allargata (o sproporzionata) di cui all'art. 240-bis c.p. ....	468
17. Concorso di norme e concorso di reati.....	470
18. Il raddoppio del termine prescrizione.....	474
19. Brevi cenni ad alcune questioni processuali.....	475
20. Responsabilità degli enti per la commissione dei delitti previsti dall'art. 600-ter c.p. ....	478

**Capitolo XI – La detenzione di materiale pedopornografico e le problematiche del web: i reati dell'art. 600-quater c.p.**

*di Stefano Delsignore*

1. Bene giuridico tutelato e natura offensiva del reato .....	487
2. Cenni di diritto comparato.....	495
3. Soggetto attivo .....	513
4. Soggetto passivo .....	514

5. Elemento oggettivo. Le condotte tipizzate dall'art. 600- <i>quater</i> c.p.: “procurarsi” e “detenere”.....	516
5.1. Procurarsi.....	516
5.2. Detenere.....	518
5.3. Oggetto materiale: il materiale pornografico realizzato utilizzando minori degli anni diciotto ed il materiale di produzione “artigianale”.....	521
6. La rilevanza della pornografia parzialmente virtuale nell'ambito delle fatispecie previste dall'art. 600- <i>quater</i> c.p. (rinvio).....	525
7. Elemento soggettivo. Il significato da attribuire all'avverbio consapevolmente.....	525
8. Individuazione del momento consumativo e configurabilità del tentativo.....	527
9. Concorso di norme e concorso di reati.....	528
10. La circostanza aggravante dell'ingente quantità, le aggravanti di cui all'art. 602- <i>ter</i> c.p., l'attenuante prevista dall'art. 600- <i>septies.1</i> c.p. e i profili sanzionatori.....	530
11. Cenni a talune questioni processuali.....	533
12. Responsabilità delle persone giuridiche per la commissione delle fatispecie previste dall'art. 600- <i>quater</i> c.p. ....	538

## **Capitolo XII – La pornografia virtuale e la lotta al “nemico” in rete. Il discrimine tra diritto penale del fatto e diritto penale d'autore**

*di Benedetta Scarcella*

1. Normativa sovranazionale ed evoluzione interpretativa.....	545
2. Profili generali.....	549
3. Interesse tutelato.....	550
4. Il concetto di “virtuale”.....	553
5. Applicazione giurisprudenziale.....	555
6. Legittimità costituzionale e questioni interpretative aperte.....	559
7. Conclusioni.....	563

## **Capitolo XIII – Sexting, minori e diritto penale**

*di Ivan Salvadori*

1. Introduzione.....	567
2. Il concetto di <i>sexting</i> .....	569
3. Gli effetti negativi del <i>sexting</i> sui minori.....	570
4. <i>Sexting</i> e pedopornografia.....	571
5. Rapporti sessuali tra e con minorenni: efficacia del consenso.....	573

6. Rilevanza penale delle condotte aventi ad oggetto pornografia minorile.....	574
6.1. Produzione di pedopornografia .....	577
6.2. Distribuzione, divulgazione, diffusione, pubblicizzazione, offerta e cessione di pedopornografia.....	581
6.3. Detenzione di pedopornografia .....	585
7. Gli orientamenti giurisprudenziali in materia di <i>sexting</i> .....	587
8. Conclusioni .....	592

## Capitolo XIV – L’adescamento di minorenni

di Michele Boggiani

1. Premessa: l’introduzione della fattispecie in esecuzione della Convenzione di Lanzarote del 2007 .....	599
2. Il bene giuridico tutelato.....	601
3. Cenni di diritto comparato: l’esempio degli Stati Uniti .....	604
4. Il soggetto attivo .....	605
5. Il soggetto passivo .....	605
6. Elemento oggettivo .....	606
7. Le note modali della condotta .....	606
8. La clausola di riserva .....	607
9. L’età del minore adescato .....	607
10. La definizione normativa di “adescamento” .....	608
11. Momento consumativo .....	610
12. Elemento soggettivo .....	610
13. La circostanza aggravante di cui all’art. 609- <i>duodecies</i> c.p.....	611
14. Pena prevista, altri aspetti sanzionatori e prescrizione .....	611
15. Rapporti con altre figure di reato.....	612

## Capitolo XV – Il *cyberstalking*

di Francesco Macrì

1. Lo <i>stalking</i> quale fenomeno criminologico e la sua incidenza statistica in Italia .....	615
2. Il delitto di “Atti persecutori” di cui all’art. 612- <i>bis</i> c.p.....	618
3. Il <i>cyberstalking</i> in generale.....	621
4. Il <i>cyberstalking</i> : profili criminologici.....	622
5. Il <i>cyberstalking</i> : la fattispecie aggravata di cui all’art. 612- <i>bis</i> , comma 2, c.p.....	626
6. Il <i>porn revenge</i> .....	627

**Capitolo XVI – Il cyberbullismo***di Maria Chiara Parmiggiani*

1. Premessa .....	631
2. Ratio della legge .....	633
3. La definizione di cyberbullismo .....	635
4. Elemento oggettivo .....	636
4.1. La molestia, l'ingiuria e la diffamazione.....	636
4.2. Il ricatto.....	638
4.3. Il furto d'identità.....	638
4.4. L'alterazione, l'acquisizione illecita e la manipolazione di dati personali.....	639
4.5. Il trattamento illecito di dati personali .....	639
4.6. La pressione, l'aggressione, la denigrazione e la diffusione di contenuti on line .....	640
5. Elemento soggettivo .....	641
6. Gli effetti del cyberbullismo .....	641
7. La tutela della persona offesa .....	642
8. Gli strumenti preventivi.....	646
9. L'ammonimento.....	647
10. Profili (provvisoriamente) conclusivi .....	649

**Capitolo XVII – I reati contro la riservatezza informatica***di Ivan Salvadori*

1. Premessa sistematica .....	656
2. Delimitazione dell'ambito dell'indagine.....	659
3. La riservatezza informatica.....	660
4. L'interrelazione tra riservatezza informatica e sicurezza informatica ....	664
5. Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) .....	666
5.1. La condotta tipica .....	667
5.2. L'abusività delle condotte di introduzione e di permanenza in un sistema informatico o telematico.....	669
5.2.1. L'abusività come perseguimento di finalità contrarie a quelle per le quali l'autorizzazione all'accesso è stata concessa .....	673
5.2.2. L'abusività quale violazione delle disposizioni che disciplinano l'introduzione o il mantenimento in un sistema informatico.....	675

5.3.	La nozione di misure di sicurezza .....	676
5.4.	L'elemento soggettivo.....	678
5.5.	Momento consumativo e tentativo.....	678
5.6.	Circostanze aggravanti.....	680
5.6.1.	L'accesso abusivo commesso da un funzionario pubblico con abuso dei poteri o violazione dei doveri o da un investigatore privato .....	680
5.6.2.	L'abuso della qualità di operatore di sistema.....	686
5.6.3.	L'accesso abusivo commesso con violenza sulle cose, alle persone o da parte di chi è palesemente armato.....	687
5.6.4.	Il danneggiamento di dati o di sistemi informatici susseguente all'accesso abusivo.....	688
5.6.5.	L'accesso abusivo a sistemi informatici di "interesse pubblico".....	689
5.7.	Struttura del reato e bene giuridico tutelato .....	689
6.	Detenzione e diffusione abusive di codici di accesso a sistemi informatici o telematici (art. 615- <i>quater</i> c.p.).....	692
6.1.	La condotta tipica .....	693
6.2.	L'abusività della condotta.....	695
6.3.	L'oggetto materiale del reato .....	697
6.4.	L'elemento soggettivo.....	698
6.5.	Momento consumativo e tentativo.....	699
6.6.	Circostanze aggravanti.....	699
6.7.	Struttura del reato e bene giuridico tutelato .....	700
7.	Diffusione di apparecchiature dirette a danneggiare un sistema informatico o telematico (art. 615- <i>quinquies</i> c.p.).....	701
7.1.	La condotta tipica .....	702
7.2.	L'oggetto materiale del reato .....	702
7.3.	L'elemento soggettivo.....	703
7.4.	Momento consumativo e tentativo.....	704
8.	Le intercettazioni informatiche e telematiche .....	704
8.1.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617- <i>quater</i> c.p.) .....	706
8.1.1.	La condotta tipica.....	706
8.1.1.1.	Il carattere fraudolento della condotta .....	708
8.1.2.	L'oggetto materiale del reato .....	709
8.1.3.	L'elemento soggettivo .....	710
8.1.4.	Momento consumativo e tentativo.....	710
8.1.5.	Circostanze aggravanti.....	710
8.1.6.	Struttura del reato e bene giuridico tutelato.....	711

8.2.	Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617- <i>quinquies</i> c.p.).....	712
8.2.1.	La condotta tipica.....	713
8.2.2.	L'oggetto materiale.....	713
8.2.3.	L'elemento soggettivo.....	714
8.2.4.	Momento consumativo e tentativo.....	714
8.2.5.	Circostanze aggravanti.....	714
8.2.6.	Struttura del reato e bene giuridico tutelato.....	715
8.3.	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617- <i>sexies</i> c.p.).....	715
8.3.1.	La condotta tipica.....	715
8.3.2.	L'oggetto materiale del reato.....	717
8.3.3.	L'elemento soggettivo.....	717
8.3.4.	Momento consumativo e tentativo.....	718
8.3.5.	Circostanze aggravanti.....	718
8.3.6.	Struttura del reato e bene giuridico tutelato.....	718
9.	La nozione di «corrispondenza» informatica o telematica.....	718

## Capitolo XVIII – “*Sex-torsion*” via *web* e minaccia a mezzo *ransomware*: la nuova frontiera del delitto di estorsione

di Mario Luberto

1.	I reati eventualmente informatici.....	724
2.	L'estorsione <i>on line</i> .....	726
3.	<i>Sex torsion</i> via <i>Web</i> ed estorsione a mezzo <i>Ransomware</i> .....	727
4.	Bene giuridico.....	731
5.	Soggetto attivo e soggetto passivo.....	732
6.	Elemento materiale.....	733
6.1.	La condotta violenta.....	734
6.2.	La condotta minacciosa.....	737
6.3.	Lo stato di coazione del soggetto passivo.....	738
6.4.	L'atto di disposizione patrimoniale coartato.....	740
6.5.	L'ingiusto profitto ed il danno altrui.....	741
7.	Elemento soggettivo.....	743
8.	Consumazione e tentativo.....	744
9.	Profili sanzionatori e circostanze aggravanti.....	748
10.	Rapporto delle <i>cyber-estorsioni</i> con altri reati.....	750
10.1.	Estorsione informatica ed esercizio arbitrario delle proprie ragioni.....	750

10.2.	Il rapporto con la violenza privata.....	752
10.3.	<i>Sex-torsion</i> via <i>web</i> e violenza sessuale.....	752
10.4.	<i>Sex-torsion</i> via <i>web</i> e reati di pedopornografia.....	754
10.5.	Estorsione a mezzo <i>Ransomware</i> ed art. 615- <i>quinq</i> ues c.p. ...	755
10.6.	Estorsione a mezzo <i>Ransomware</i> e danneggiamento informatico.....	757

## Capitolo XIX – I delitti contro l’integrità dei dati, dei programmi e dei sistemi informatici

di Alberto Cappellini

1.	Introduzione.....	762
2.	Evoluzione e quadro della normativa.....	767
2.1.	La riforma del 1993.....	768
2.2.	Gli impulsi internazionali e la riforma del 2008.....	772
2.3.	Gli interventi operati dal D.Lgs. 15.1.2016, n. 7, in tema di depenalizzazioni.....	775
3.	I delitti di danneggiamento di dati e sistemi “privati” (artt. 635- <i>bis</i> e 635- <i>quater</i> c.p.).....	776
3.1.	Il soggetto attivo.....	777
3.2.	Gli oggetti materiali.....	778
3.3.	Le condotte.....	783
3.4.	Gli eventi.....	788
3.5.	L’elemento soggettivo.....	793
3.6.	La consumazione e il tentativo.....	793
3.7.	Le circostanze aggravanti specifiche.....	793
3.8.	Rapporti tra reati.....	795
3.9.	Profili sanzionatori e processuali.....	797
4.	I delitti di danneggiamento di dati e sistemi “pubblici” (artt. 635- <i>ter</i> e 635- <i>quinq</i> ues c.p.).....	798
4.1.	Il soggetto attivo.....	800
4.2.	Gli oggetti materiali.....	800
4.3.	Le condotte.....	802
4.4.	L’elemento soggettivo.....	804
4.5.	La consumazione e il tentativo.....	805
4.6.	Gli eventi aggravatori.....	805
4.7.	Le circostanze aggravanti specifiche.....	806
4.8.	Rapporti tra reati.....	807
4.9.	Profili sanzionatori e processuali.....	808
5.	Il delitto di diffusione di apparecchiature, dispositivi o programmi nocivi (art. 615- <i>quinq</i> ues c.p.).....	809

5.1.	Il soggetto attivo .....	810
5.2.	Gli oggetti materiali.....	810
5.3.	Le condotte .....	813
5.4.	L'elemento soggettivo.....	814
5.5.	La consumazione e il tentativo .....	816
5.6.	Rapporti tra reati.....	817
5.7.	Profili sanzionatori e processuali.....	818
6.	L'equiparazione della "violenza informatica" alla violenza sulle cose (art. 392, ultimo comma, c.p.) .....	818

## Capitolo XX – Le frodi informatiche

*di Gherardo Minicucci*

1.	Il delitto di frode informatica (art. 640-ter c.p.) .....	827
1.1.	Il soggetto attivo .....	830
1.2.	La condotta .....	830
1.3.	Gli eventi.....	836
1.4.	L'elemento soggettivo.....	837
1.5.	La consumazione e il tentativo .....	837
1.6.	Le circostanze aggravanti speciali.....	838
1.7.	La truffa a mezzo <i>web</i> .....	840
1.8.	Il <i>phishing</i> .....	841
1.9.	Rapporti tra reati.....	842
1.10.	Profili sanzionatori e processuali. Le confische.....	845
2.	Il delitto di frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).....	849
2.1.	Il soggetto attivo .....	850
2.2.	La condotta .....	850
2.3.	L'elemento soggettivo.....	852
2.4.	La consumazione e il tentativo .....	854
2.5.	Rapporti tra reati.....	854
2.6.	Profili sanzionatori e processuali. La confisca.....	854

## Capitolo XXI – Il cybericiclaggio

*di Vito Plantamura*

1.	Il riciclaggio e il reimpiego .....	859
1.1.	L'autoriciclaggio.....	864
2.	Il <i>cybericiclaggio</i> .....	871
3.	Il <i>cybericiclaggio</i> e la criminalità organizzata.....	874
3.1.	In particolare: il finanziamento del terrorismo.....	877

4. Il <i>cybericiclaggio</i> e le valute virtuali .....	880
5. Il <i>cybericiclaggio</i> e il <i>gambling online</i> .....	884
6. Conclusioni .....	886

**Capitolo XXII – Riservatezza e diritto alla *privacy*: in particolare, la responsabilità per *omissionem* dell’*internet provider***

*di Adelmo Manna e Mattia Di Florio*

1. Riservatezza e diritto alla <i>privacy</i> : profili generali.....	892
2. Il delitto di trattamento illecito di dati personali (art. 167 Cod. <i>privacy</i> ).....	896
2.1. L’art. 167 del Codice della <i>privacy</i> e il problema relativo alla responsabilità penale dell’ <i>internet provider</i> : il caso <i>Google-Vivi Down</i> .....	901
2.2. (Segue) Ulteriore sviluppo della giurisprudenza della Cassazione in materia di responsabilità penale dell’ <i>internet provider</i> : pregi e limiti.....	909
3. La sicurezza informatica: il reato contravvenzionale di omessa adozione di misure minime di sicurezza nei trattamenti elettronici di dati personali (art. 169 Cod. <i>privacy</i> ).....	916
4. I reati contro il diritto alla <i>privacy</i> “informatica” del lavoratore: l’art. 171 Cod. <i>Privacy</i> .....	923
4.1. (Segue)... e i reati del Codice penale a tutela delle comunicazioni informatiche.....	930
5. Postilla: le novità apportate dal GDPR ( <i>General Data Protection Regulation</i> ).....	935
5.1. (Segue) Le novità apportate dal D.Lgs. 18.5.2018, n. 51 recante attuazione della Direttiva 2016/680/UE sul trattamento dei dati personali in ambito penale.....	937

**Capitolo XXIII – Gli obblighi dei fornitori di servizi di comunicazione elettronica in caso di violazione dei dati personali (*data breach*) ed il delitto dell’art. 168, D.Lgs. n. 196/2003**

*di Mario Luberto*

1. Premessa .....	942
2. Gli obblighi di comunicazione da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico e di altri soggetti in caso di violazione della sicurezza dei dati personali (art. 32- <i>bis</i> , D.Lgs. 30.6.2003, n. 196).....	944
3. Le sanzioni amministrative (art. 162- <i>ter</i> , D.l.gs. 30.6.2003, n. 196) ....	952

4. Il delitto di falsità nella comunicazione al Garante in caso di <i>data breach</i> (art. 168, D.Lgs. 30.6.2003, n. 196 in relazione all'art. 32- <i>bis</i> ) .....	953
5. Gli obblighi in caso di <i>data breach</i> nel Reg. 2016/679/UE sulla protezione dei dati personali.....	963
6. La falsità nelle dichiarazioni al Garante e l'adeguamento dell'ordinamento giuridico italiano al Reg. 2016/679/UE. Dagli schemi di decreto al D.Lgs. 10.8.2018, n. 101 .....	967

## **Capitolo XXIV – Il sistema delle tutele nel regolamento europeo n. 679/2016 sulla protezione dei dati personali**

*di Daniele Labianca*

1. Introduzione.....	978
2. Il Regolamento privacy europeo del 2016. Genesi e precedenti .....	979
3. (Segue) La struttura del Regolamento. I diritti dell'interessato .....	983
4. I mezzi di tutela dell'interessato .....	992
4.1. (Segue) Il ricorso in via amministrativa all'autorità di controllo (art. 77).....	993
4.2. (Segue) Il ricorso avverso un provvedimento dell'autorità (art. 78).....	994
4.3. (Segue) L'impugnazione delle decisioni del Comitato europeo per la protezione dei dati .....	996
4.4. (Segue) La tutela giurisdizionale nei confronti del titolare del trattamento o del responsabile del trattamento.....	997
5. La tutela risarcitoria.....	998
6. L'apparato sanzionatorio amministrativo .....	1000
7. La facoltà per gli Stati membri di adottare "altre" sanzioni. Le sanzioni penali ed il principio del <i>ne bis in idem</i> .....	1004
8. L'interferenza della disciplina eurounitaria con la normativa italiana. L'adeguamento dell'ordinamento interno: il D.Lgs. n. 101/2018 .....	1010

## **Capitolo XXV – I reati in materia di protezione dei dati personali**

*di Federica Resta*

1. I reati previsti dal decreto legislativo di recepimento della Dir. (UE) 2016/680 .....	1020
1.1. Profili generali .....	1020
1.2. Le fattispecie di reato .....	1024
1.2.1. Trattamento illecito .....	1024
1.2.2. Falsità in atti e dichiarazioni al Garante .....	1025

1.2.3.	Inosservanza di provvedimenti del Garante.....	1026
1.2.4.	Gli illeciti commessi nel contesto dell' <i>intelligence</i> ....	1026
2.	I reati previsti dal decreto legislativo di adeguamento dell'ordinamento interno al Reg. (UE) 2016/679 .....	1027
2.1.	L'evoluzione della disciplina proposta, sino all'invio del testo alle Camere per il parere.....	1027
2.2.	L'evoluzione della disciplina, dal testo proposto alle Camere a quello definitivo .....	1029
2.2.1.	Linee generali.....	1029
2.2.2.	Il rischio di violazione del <i>ne bis in idem</i> .....	1031
2.3.	Il trattamento illecito di dati personali .....	1034
2.4.	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala .....	1036
2.5.	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala .....	1040
2.6.	Disposizioni ulteriori .....	1041

## Capitolo XXVI – La tutela penale dei diritti d'autore e connessi

di Roberto Flor

1.	Premessa .....	1046
2.	Percorsi storici .....	1050
3.	Le più recenti fonti internazionali ed europee (cenni).....	1056
4.	La tutela penale dei diritti d'autore in Italia .....	1061
5.	I "caratteri generali" del sistema di tutela penale del diritto d'autore e dei diritti connessi.....	1063
6.	La struttura "complessa" delle fattispecie legali e rapporti fra reati previsti da articoli diversi della l.d.a. e con altri reati "esterni" al micro-sistema penale di tutela dei diritti d'autore.....	1077
7.	Le principali fattispecie penali previste dalla l.d.a .....	1094
7.1.	Art. 171 l.d.a .....	1095
7.2.	Art. 171- <i>bis</i> l.d.a .....	1097
7.2.1.	La duplicazione abusiva di un programma per elaboratore.....	1102
7.2.2.	L'elemento finalistico della fattispecie e l'interpretazione sistematica con la detenzione a scopo commerciale o imprenditoriale di programmi per elaboratore contenuti in supporti non contrassegnati dalla SIAE.....	1108
7.2.3.	La tutela penale delle banche dati.....	1121

7.2.3.1.	La definizione di banca dati e l'attuazione della normativa europea .....	1121
7.2.3.2.	Opere multimediali e banche dati: profili penalistici.....	1124
7.2.3.3.	Banche dati, diritti d'autore e fattispecie incriminatrice.....	1126
7.3.	Art. 171-ter l.d.a .....	1129
7.3.1.	La rilevanza penale dell'“immissione” abusiva, in un sistema di reti telematiche, di un'opera dell'ingegno protetta dai diritti d'autore .....	1131
7.3.2.	I più recenti e frequenti casi di applicazione dell'art. 171-ter l.d.a .....	1139
7.4.	Tutela penale e autotutela tecnologica dei diritti d'autore .....	1141
8.	L'art. 171-octies l.d.a. e la questione di incostituzionalità .....	1150
9.	L'art. 171-octies.1 e l'art. 171-nonies l.d.a.....	1152
10.	La responsabilità dell' <i>Internet Service Provider</i> per le violazioni penali dei diritti d'autore (cenni).....	1154
11.	Beni giuridici protetti e progresso culturale, sociale ed economico.....	1165
12.	Le “tendenze” europee: il ruolo propulsore della Corte di Giustizia e l'evoluzione delle tutele dei diritti d'autore (cenni) .....	1170

### Parte III

#### Diritto penale sostanziale: nuove frontiere

##### Capitolo I – *Robot, cyborg e intelligenze artificiali*

di Maria Beatrice Magro

1.	I robot intelligenti .....	1180
1.1.	Questioni e spunti di riflessione in tema di Intelligenze artificiali.....	1180
1.2.	La sfida della Intelligenza Artificiale generale o forte: robotica e neuroscienze cognitive.....	1182
1.3.	A favore di una proficua e utile complementarietà tra umani e macchine .....	1186
2.	Bio-robotica, <i>Cybor</i> e sistemi di <i>Interfaces Brain Machine</i> : dall' <i>Homo Sapiens</i> all' <i>Homo Deus</i> .....	1187
3.	Distinzione tra <i>robot</i> , Agenti intelligenti e robot intelligenti .....	1190
4.	I campi di applicazione della Robotica evoluta.....	1192
5.	Verso una Superintelligenza artificiale? .....	1194

5.1.	Intelligenza, razionalità e senso comune.....	1194
5.2.	La coscienza artificiale dei <i>Robot</i> .....	1196
6.	Questioni di Robotetica .....	1197
6.1.	La Roboetica e le leggi della robotica .....	1197
6.2.	L'etica umani-robot .....	1198
6.3.	L'etica robot-umani .....	1199
6.4.	Le scelte etiche nella programmazione e nel design.....	1200
7.	I robot intelligenti: oggetti o soggetti giuridici?.....	1201
7.1.	Lo statuto ontologico delle macchine.....	1201
7.2.	I <i>robot</i> intelligenti godono di autonomia e di libertà di agire? Possono essere considerati soggetti in senso giuridico? .....	1202
7.3.	I <i>robot</i> hanno capacità criminale? .....	1203
7.4.	I <i>robot</i> possono subire sanzioni penali? .....	1204
8.	Questioni giuridiche .....	1205
8.1.	La normativa europea .....	1205
8.2.	Se i <i>robot</i> sono mezzi (e non agenti): la responsabilità del programmatore o utilizzatore a titolo di dolo.....	1206
8.3.	La colpa del programmatore per non aver previsto l'imprevedibile.....	1207
8.4.	Il problema della prevedibilità dei comportamenti dei sistemi robotici intelligenti. I rischi dell'innovazione tecnologica.....	1209
8.5.	Conclusioni.....	1211

## Capitolo II – Potenziamiento cognitivo e diritto penale

di Odette Eronia

1.	Generalità.....	1213
2.	Il miglioramento delle funzioni cerebrali. Realtà o finzione? Qualche dato statistico .....	1219
3.	Potenziamiento cognitivo e diritto penale: “labili intersezioni”.....	1225
3.1.	La <i>super</i> -salute.....	1226
3.2.	Il consenso “ <i>super</i> -informato” .....	1230
3.3.	La <i>super</i> -responsabilità del medico.....	1236
4.	“Timide aperture” nel Codice di Deontologia medica: l'art. 76 e la medicina potenziativa .....	1242
5.	Nuove frontiere: “App” della salute, farmacie <i>on line</i> e <i>Dark Web</i> .....	1245
6.	Conclusioni: scenari di “neuro-civilizzazione”? .....	1248

### Capitolo III – I progetti di legge sulle *fake news* e la disciplina tedesca a confronto

di Pierluigi Guercia

1. Sintetiche riflessioni prodromiche: le <i>fake news</i> nell'epoca della "post-verità" .....	1254
2. I tentativi di regolamentazione normativa in Italia: " <i>fake news</i> " o " <i>fake laws</i> "? .....	1257
2.1. Il c.d. "D.d.l. Gambaro" .....	1258
2.2. Il progetto Zanda-Filippin e l'influente impatto della "soluzione tedesca" .....	1263
3. Le ultime pagine di una storia ancora tutta da scrivere: il modello " <i>red button</i> " all'italiana .....	1268

### Capitolo IV – *Cyberwarfare*: gli scenari della guerra informatica

di Mario L'Insalata

1. Informatica e minacce dell'Era moderna .....	1273
2. Definizione di " <i>cyberwarfare</i> " .....	1277
2.1. Tipi di <i>cyberwarfare</i> .....	1279
2.2. Finalità della <i>cyberwarfare</i> .....	1281
2.3. Modalità attuative .....	1282
2.3.1. Spionaggio .....	1282
2.3.2. Sabotaggio .....	1283
2.3.3. Guerra psicologica .....	1286
2.3.4. Dissuasione .....	1287
2.4. Pubblicità o segretezza degli atti di <i>cyberwarfare</i> .....	1287
2.5. <i>Cyberdefence</i> .....	1287
3. Modalità operative di <i>cyberwarfare</i> e loro riconducibilità a fattispecie dell'ordinamento penale italiano .....	1289
4. La giurisdizione sulle condotte di <i>cyberwarfare</i> .....	1295
5. La normativa italiana ed europea per la difesa dagli attacchi informatici .....	1296

## Parte IV

### Diritto processuale penale

#### Capitolo I – Le prove informatiche

di Giorgio Spangher

**Capitolo II – L’evoluzione delle categorie tradizionali: il documento informatico**

*di Paolo Tonini*

1. Il documento informatico: categorie civilistiche e penalistiche .....	1308
2. L’informatica come presunta forma di rappresentazione di un fatto....	1309
3. L’informatica come forma di incorporamento della rappresentazione di un fatto .....	1311
4. Il documento informatico tra immaterialità e dematerializzazione.....	1312
5. La definizione di documento informatico .....	1314
6. Documento informatico e contraddittorio .....	1316
7. L’estrazione della copia di un <i>file</i> dal <i>computer</i> .....	1316
8. La non ripetibilità nell’informatica forense.....	1319
9. La correlazione tra la definizione di documento informatico e la forma di acquisizione del medesimo.....	1319
10. Considerazioni sul concetto di non ripetibilità.....	1320
11. Non ripetibilità e riforma dell’art. 111 Cost.....	1322
12. Non ripetibilità e nucleo insopprimibile del contraddittorio .....	1324
13. La tutela del contraddittorio <i>ex post</i> .....	1325

**Capitolo III – La prova informatica e il mancato rispetto della *best practice*: lineamenti sistematici sulle conseguenze processuali**

*di Carlotta Conti*

1. Nuovi paradigmi .....	1329
2. L’insufficienza del contraddittorio contestuale o postumo.....	1331
3. <i>Forma essentialis</i> e inutilizzabilità tra <i>an</i> e <i>quomodo</i> .....	1334
4. Tre modelli di eterointegrazione dei divieti.....	1337
5. La ricostruzione in punto di regole di valutazione .....	1342
6. L’onere della prova .....	1344
7. Considerazioni conclusive .....	1346

**Capitolo IV – La convenzione di Budapest del 2001 e la L. n. 48/2008**

*di Stefano Aterno*

1. Premessa .....	1351
2. La L. n. 48/2008 in generale e alcuni aspetti tecnico giuridici fondamentali .....	1354
3. L’accertamento tecnico urgente sui supporti informatici .....	1363
4. La custodia delle cose sequestrate <i>ex art.</i> 259 c.p.p. ....	1366

5. Il sequestro di corrispondenza inoltrata per via telematica <i>ex art.</i> 254 c.p.p.....	1368
6. Atti ripetibili e atti irripetibili .....	1371

## Capitolo V – Le ispezioni e perquisizioni di dati e sistemi

*di Paola Felicioni*

1. Ispezioni e perquisizioni tra evoluzione tecnologica ed evoluzione normativa .....	1377
2. Ispezione e perquisizione informatiche: profili definitivi .....	1382
2.1. La nozione .....	1382
2.2. L'oggetto della ricerca ispettiva e perquirente .....	1387
2.3. L'oggetto investito dalla ricerca probatoria: sistemi informatici o telematici.....	1391
2.4. Il labile discrimine tra ispezione informatica e perquisizione informatica.....	1394
2.5. La copia forense come tecnica di ricerca o come accertamento autonomo: rinvio.....	1399
3. Ricerca della prova informatica e diritti fondamentali.....	1400
3.1. I diritti dell'individuo .....	1400
3.2. I diritti processuali .....	1404
4. La dinamica probatoria: ricognizione normativa e profili di specialità... ..	1408
4.1. La motivazione del provvedimento .....	1408
4.2. Le procedure di <i>computer forensics</i> : individuazione del reperto, acquisizione e analisi dei dati digitali.....	1412
4.3. Le modalità esecutive .....	1423
4.4. L'esame di dati, informazioni e programmi informatici presso banche .....	1428
4.5. Le garanzie difensive.....	1429

## Capitolo VI – Il sequestro di dati e sistemi

*di Alessandra Testaguzza*

1. Il valore della prova informatica nel processo penale .....	1437
2. La Convenzione di Budapest e i nuovi mezzi di ricerca della prova.....	1439
3. Le <i>best practices</i> nelle indagini informatiche .....	1442
4. Il sequestro probatorio di dati e sistemi informatici.....	1446
5. La dubbia natura giuridica dei sequestri di dati e sistemi .....	1449
6. Il sequestro di siti <i>web</i> e delle testate giornalistiche <i>online</i> .....	1451
7. Alcuni aspetti problematici.....	1456

**Capitolo VII – L’intercettazione di flussi telematici (art. 266-bis c.p.p.)**

*di Marco Torre*

1. Il concetto di intercettazione telematica .....	1463
2. L’intercettazione dei messaggi di posta elettronica .....	1466
2.1. Le “cartelle” di posta elettronica .....	1468
3. L’intercettazione delle <i>chat</i> .....	1470
4. L’intercettazione delle comunicazioni <i>VoIP</i> .....	1472

**Capitolo VIII – L’accertamento tecnico ripetibile. La gestione del reperto informatico**

*di Vincenzo Lagi*

1. Introduzione.....	1477
2. Il dato informatico .....	1479
3. Le fasi dell’accertamento.....	1481
4. Ripetibilità e <i>best practices</i> .....	1484
5. Conclusioni.....	1487

**Capitolo IX – Le indagini di *digital forensics* di iniziativa della polizia giudiziaria**

*di Marco Torre*

1. Premessa .....	1489
2. Il trattamento forense dell’evidenza digitale .....	1492
3. Le <i>best practices</i> nelle investigazioni informatiche .....	1493
3.1. Individuazione della fonte di prova .....	1495
3.2. Acquisizione dei dati .....	1496
3.3. Conservazione dell’evidenza digitale.....	1503
3.4. Analisi dei dati e presentazione dei risultati.....	1505
4. Il c.d. potere tecnico-investigativo.....	1506

**Capitolo X – La competenza della procura distrettuale per i reati informatici**

*di Francesco Cajani*

1. Premessa: i lavori parlamentari della L. 18.3.2008, n. 48.....	1511
2. Il testo della Convenzione di Budapest in punto di giurisdizione e l’assenza di alcune indicazioni in materia di competenza.....	1513
3. I reati rientranti nella competenza c.d. distrettuale.....	1514
4. Regime intertemporale .....	1515

5. La *vis attractiva* dei procedimenti relativi ai reati c.d. distrettuali rispetto ai procedimenti relativi ad altri reati ad esso connessi ..... 1516
6. Alcune osservazioni critiche sulla previsione di una competenza territoriale distrettuale per i *computer crimes* ..... 1517

**Capitolo XI – Le indagini informatiche per i reati di *cyberterrorismo***  
di Francesco Cajani

1. Preambolo ..... 1522
2. L'evoluzione della normativa in materia di terrorismo e l'ascesa delle nuove tecnologie ..... 1523
3. La nozione di *cyberterrorismo* ..... 1524
  - 3.1. (Segue) L'ambito di applicazione delle normative in materia di *cybercrime* e terrorismo ..... 1528
4. L'eterno problema della *data retention* e i rapporti con gli *Internet Service Provider* ..... 1529
5. Il terror(ismo) che si propaga al ritmo dell'*instant messaging* ..... 1535
  - 5.1. L'avvento del *trojan* quale imprescindibile strumento d'indagine per far fronte a una duplice difficoltà investigativa: lo stato attuale delle intercettazioni di comunicazioni tramite sistemi VoIP (comprensivi oggi dei sistemi di *istant messaging*) con protocolli di crittografia e delle caselle di posta elettronica *@.com* ..... 1540
6. Il monitoraggio della Rete e il tempestivo intervento di rimozione dei contenuti illeciti *online* ..... 1544
7. Casi di accessi transfrontalieri a dati informatici: una prospettiva legale ..... 1546
8. Quali previsioni per un futuro ancora incerto? ..... 1548

**Capitolo XII – Le indagini informatiche per reati di pedopornografia *online*: tra esigenze di accertamento e tutela dei diritti fondamentali**  
di Eleonora Addante

1. Premessa: le coordinate spazio-temporali digitali ..... 1553
2. I reati di pedopornografia *online* e le indagini informatiche: tra comode astrattezze e bisognose concretezze ..... 1556
3. Le attività di contrasto “digitali” ex art. 14, L. n. 269/1998 ..... 1560
4. Il rispetto dei limiti normativi quale *condicio sine qua non* per la legittimità delle operazioni *under cover* ..... 1565
5. Utilizzabilità o non utilizzabilità del materiale probatorio? Questo è il dilemma ..... 1568

5.1. Le attività di contrasto nell’ambito europeo: utili spunti di riflessione.....	1572
6. Conclusione: la necessità di un intervento legislativo come argine agli abusi degli strumenti processuali.....	1574

**Capitolo XIII – L’istituto della *data retention* dopo la sentenza della Corte di Giustizia del 2014**

*di Stefano Marcolini*

1. La descrizione tecnica del fenomeno e le libertà fondamentali incise ...	1579
2. L’attuale disciplina di diritto interno: l’art. 132 Codice <i>privacy</i> .....	1582
3. Lo “tsunami” comunitario ...	1586
4. ... e le reazioni interne. Prospettive.....	1590

**Capitolo XIV – Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati**

*di Gian Marco Baccari*

1. Premesse .....	1599
2. La <i>data retention</i> nel codice della <i>privacy</i> del 2003 .....	1603
3. I termini di conservazione dei dati e la procedura di acquisizione.....	1605
4. La dichiarazione di invalidità della Dir. 2006/24 da parte della Corte di Giustizia europea.....	1607
5. La disciplina italiana della <i>data retention</i> dopo le misure antiterrorismo del 2015 e del 2017.....	1609
6. Le principali novità del D.Lgs. n. 51/2018 di attuazione della Dir. 2016/680/UE.....	1611
7. Il recente Regolamento sul trattamento dei dati personali da parte delle forze di polizia .....	1614

**Capitolo XV – La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche**

*di Marcello Daniele*

1. Dalla rogatoria all’ordine europeo di indagine penale .....	1621
2. La raccolta delle prove digitali <i>in loco</i> .....	1622
2.1. L’emissione della richiesta di raccolta della prova.....	1623
2.2. Il rifiuto .....	1624
2.3. L’esecuzione .....	1627
2.4. L’utilizzabilità della prova.....	1630
3. La raccolta delle prove digitali a distanza .....	1632

3.1.	L'acquisizione diretta di dati non riservati .....	1632
3.2.	L'acquisizione diretta di dati riservati .....	1633
3.3.	Le intercettazioni informatiche transnazionali .....	1635

## **Capitolo XVI – La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno *standard***

*di Maria Angela Biasiotti, Sara Conti, Fabrizio Turchi*

1.	Introduzione .....	1639
2.	Natura transnazionale della prova digitale .....	1641
3.	Il quadro giuridico dell'Unione europea in materia di cooperazione giudiziaria penale per lo scambio delle prove digitali .....	1642
4.	Le iniziative operative delle Istituzioni europee .....	1648
5.	Spunti per la realizzazione di un quadro comune europeo in materia di scambio delle prove digitali .....	1652
6.	Scambio di prove digitali: una proposta di standard .....	1654
7.	Conclusioni e prospettive future .....	1656

## **Capitolo XVII – Le intercettazioni a mezzo del c.d. *captatore informatico o "trojan di Stato"***

*di Marco Torre*

1.	Premessa .....	1660
2.	Le intercettazioni di conversazioni tra presenti mediante captatore informatico .....	1661
2.1.	Limiti di ammissibilità .....	1663
2.2.	Presupposti e forme del provvedimento di autorizzazione .....	1665
2.3.	Esecuzione delle operazioni e verbalizzazione delle intercettazioni .....	1667
2.4.	Regime di utilizzabilità .....	1669
2.5.	La tutela della riservatezza .....	1670
3.	La poliedricità del captatore informatico: perquisizioni <i>on line</i> e <i>keylogger software</i> .....	1671
4.	Conclusioni .....	1673

## **Capitolo XVIII – Sull'obbligo per il privato di collaborare ad attività di *digital forensics*: il caso "Apple – F.B.I."**

*di Marco Torre*

1.	Il fatto .....	1676
2.	La <i>querelle</i> giudiziaria .....	1678

3. La c.d. servitù di giustizia in Italia: sicurezza pubblica vs diritti individuali .....	1682
4. Prerogative pubbliche vs poteri privati .....	1686

**Capitolo XIX – Cloud forensics: aspetti giuridici e tecnici**

*di Stefano Aterno*

1. Definizione teorica ed implementazioni reali dei <i>cloud system</i> .....	1689
1.1. Struttura e tipi di servizi <i>Cloud</i> .....	1692
1.2. Sopralluogo e repertamento sui <i>Cloud</i> .....	1694
2. Quali norme e garanzie in tema di ispezione, perquisizione e sequestro in ambiente <i>cloud computing</i> ? .....	1696
3. Il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni <i>ex art. 254-bis c.p.p.</i> : quando i dati sono su <i>Cloud</i> .....	1701
4. L'art. 234- <i>bis</i> . Acquisizione di documenti e dati informatici presenti all'estero: il caso dell'acquisizione su piattaforme di <i>cloud system</i> .....	1702

**Capitolo XX – Deep web, dark web e indagini informatiche**

*di Vincenzo Lagi*

1. Introduzione .....	1707
2. L'ambito del <i>deep web</i> .....	1708
3. Il sottoinsieme del <i>dark web</i> .....	1710
4. Possibili tecniche investigative .....	1711
5. Conclusioni .....	1711

<b>Indice analitico</b> .....	1713
-------------------------------	------

*A cura di Alberto Cappellini*



L'estratto che stai visualizzando  
è tratto da un volume pubblicato su  
ShopWki - La libreria del professionista

[VAI ALLA SCHEDA PRODOTTO](#)