

L'estratto che stai consultando
fa parte del volume in vendita
su **ShopWKI**,
il negozio online di **Wolters Kluwer**

[Torna al libro](#)



CEDAM

IPSOA

UTET[®]
GIURIDICA

il fisco

 ALTALEX

INDICE SISTEMATICO

Indice degli autori	XXXVII
Presentazione	XLIII
<i>di Michele Papa</i>	

Parte I

Diritto penale sostanziale: questioni e prospettive di fondo

Capitolo I - Profili tecnico-informatici e filosofici 2.0

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	28

Capitolo II - Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme

di Lorenzo Picotti

1. La rivoluzione tecnologica ed il suo impatto sui rapporti sociali e giuridici	32
1.1. Mutamenti indotti dallo sviluppo tecnologico, "rivoluzione" cibernetica ed intelligenza artificiale	34
1.2. Dalla Rete al <i>Cyberspace</i>	36
1.3. Reciprocità di condizionamento fra tecnologia e diritto	38
2. Rilevanza giuridico-penale dell'automazione e dell'intelligenza artificiale quale "sostituzione" (parziale) dell'attività e della volontà dell'uomo	42
3. Il passaggio dai <i>Computer crime</i> ai <i>Cybercrime</i> fino agli <i>AI-crime</i>	46
4. Il <i>web</i> interattivo ed il doppio ruolo degli utenti quali possibili autori e vittime di reati cibernetici	57

5.	Tecniche di tipizzazione dei reati informatici e cibernetici e relative partizioni classificatorie.....	60
5.1.	Nuove condotte, estensioni “analogiche”, nuovi oggetti materiali.....	60
5.1.1.	Nuove condotte e nuovi “fatti” di reato: in particolare le fattispecie paradigmatiche della frode informatica e dell’accesso abusivo	61
5.1.2.	Estensioni per “analogia” legislativa di fattispecie preesistenti a nuovi oggetti “materiali” e relative modalità di condotta	67
5.2.	Collocazione sistematica e beni giuridici protetti	73
5.3.	Partizioni dei reati informatici e cibernetici ovvero realizzati tramite sistemi di intelligenza artificiale.....	76
5.3.1.	I reati informatici in senso stretto	76
5.3.2.	I reati informatici in senso ampio.....	77
5.3.3.	Reati cibernetici.....	79
5.3.4.	Sulla responsabilità penale per fatti di reato commessi tramite sistemi di intelligenza artificiale	81
5.4.	Spunti conclusivi	86
6.	Obblighi di tutela penale degli <i>Internet Service Providers</i> e dei titolari di piattaforme digitali: sviluppi della giurisprudenza e della normativa europea.....	87
6.1.	Giurisprudenza Corte EDU.....	90
6.2.	Giurisprudenza C. Giust. UE	92
6.3.	Recenti sviluppi della normativa europea.....	94
7.	Osservazioni conclusive: verso un’evoluzione di categorie tradizionali della teoria del reato alla luce degli sviluppi tecnologici	98

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

di Roberto Flor

	Premessa metodologica	108
1.	Le fonti internazionali ed il sistema interno: dagli “albori” del diritto penale dell’informatica alla Convenzione <i>Cybercrime</i>	108
2.	Le fonti UE <i>ante</i> Lisbona.....	117
3.	Le fonti UE <i>post</i> Lisbona.....	125
4.	Uno sguardo necessario al ruolo “propulsore” della Corte di Giustizia .	135
4.1.	Il caso “Google/Spain”	137
4.2.	La prima sentenza della Corte di Giustizia sulla c.d. <i>data retention</i> e la successiva evoluzione giurisprudenziale europea (cenni) un importante passo per il rafforzamento del diritto	

alla riservatezza. Ma con quali effetti per il sistema di giustizia penale?.....	140
5. <i>Last but not least</i> : il regolamento europeo in materia di protezione dei dati personali, la Dir. 2016/680/UE, il <i>Cybersecurity Act</i> e la proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (rinvio)	144

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

di Roberto Flor

1. Introduzione.....	154
2. Prima premessa di ordine generale: il diritto penale italiano.....	156
3. Seconda premessa di ordine generale: la Convenzione <i>Cybercrime</i>	159
4. Terza premessa di ordine generale: le fonti europee.....	160
5. Il <i>locus commissi delicti</i> nel <i>cyberspace</i>	162
5.1. Il caso della diffamazione	166
5.2. Il caso delle truffe <i>online</i>	173
5.2.1. (Segue) Le ipotesi di truffa comune realizzata attraverso l'utilizzo di strumenti tecnologici o la rete.....	174
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.....	180
5.3. Il caso dell'accesso abusivo a sistemi informatici o telematici	187
6. Considerazioni di sintesi	203

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

di Désirée Fondaroli

1. Premessa.....	209
2. La responsabilità degli enti ex D.Lgs. n. 231/2001.....	210
3. I reati informatici, presupposto della responsabilità degli enti	217
4. <i>Privacy</i> e D.Lgs. n. 231/2001	222

Parte II

Diritto penale sostanziale: tematiche di carattere specifico

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

di Stefano Dambruoso, con la collaborazione, in fase di ricerca, di Greta Gjuzi e Francesco Conti

1. Inquadramento	229
2. Addestramento ad attività con finalità di terrorismo anche internaziona- le	230
3. Istigazione e apologia di terrorismo	232

Capitolo II - L'istigazione a delinquere via web

di Michele Boggiani, rivisto e aggiornato da Francesca Manfredi

1. Introduzione.....	237
2. Bene giuridico protetto: l'ordine pubblico e i beni finali dei delitti og- getto di istigazione e di apologia	238
3. Il soggetto attivo.....	239
4. Elemento oggettivo: in particolare, la compatibilità delle condotte isti- gatrici e apologetiche con l'art. 21 Cost.	239
5. (Segue) La pubblicità della condotta.....	241
6. (Segue) I destinatari della condotta.....	242
7. (Segue) Le circostanze aggravanti di cui al comma 3 e al comma 4 – commissione del fatto attraverso strumenti informatici o telematici.....	243
8. Elemento soggettivo	244
9. La pena prevista	244
10. Rapporti con altre figure di reato	245

Capitolo III - Istigazione a pratiche di pedofilia e di pedopornografia

di Malaika Bianchi

1. <i>Ratio</i> della norma e bene giuridico tutelato	249
2. Elemento oggettivo	253
3. Elemento soggettivo	255
4. La non scusabilità delle ragioni o finalità di carattere artistico, letterario, storico o di costume.....	256
5. Consumazione e tentativo	258
6. Rapporti con altri reati	258
7. Norma superflua o necessaria? Incriminazione compatibile con il di- ritto alla libertà di manifestazione del pensiero? Riflessioni conclusive dopo dieci anni dalla sua introduzione	258

Capitolo IV - L'associazione per delinquere "informatica"*di Nicolò Bussolati*

1. I sodalizi criminosi e la rete	261
2. L'associazione per delinquere informatica nel quadro normativo esistente	264
3. Le particolarità morfologiche delle comunità virtuali.....	267
4. Le associazioni per delinquere finalizzate allo scambio di materiale pedopornografico.....	269
5. Le associazioni per delinquere finalizzate agli attacchi informatici.....	274

Capitolo V - Le falsità informatiche*di Giandomenico Salcuni*

1. Premessa.....	285
2. Questioni intertemporali	287
3. Soggetto attivo ed elemento soggettivo.....	288
4. La condotta	288
5. Oggetto materiale	291
6. Forme di manifestazione del reato	293

Capitolo VI - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*di Andrea Galante*

1. L'origine e lo scopo della tutela penale degli strumenti di pagamento diversi dai contanti	297
2. L'evoluzione della tutela a seguito dello sviluppo dei sistemi di pagamento	300
3. L'oggetto materiale della tutela: carte di credito, di pagamento, documenti analoghi e altri strumenti di pagamento diversi dai contanti.....	302
4. L'indebito utilizzo di strumenti di pagamento diversi dai contanti	306
5. La falsificazione o alterazione di strumenti di pagamento	313
6. Il possesso, la cessione o l'acquisizione di strumenti di pagamento di provenienza illecita.....	315

Capitolo VII - La sostituzione di persona mediante furto di identità digitale*di Marisa Marraffino*

1. Premesse.....	321
2. Il bene giuridico protetto dalla norma e gli elementi costitutivi del reato	325
3. L'elemento soggettivo	330

4. Il phishing e le nuove falsificazioni digitali	331
5. False identità virtuali e Reg. UE 2016/679	333
6. Acquisizione delle prime evidenze digitali e problemi esecutivi.....	335
7. Profili amministrativi: l'azione davanti al Garante per la protezione dei dati personali.....	337
8. Le possibili responsabilità del fornitore di servizi legate al furto di identità.....	339
9. Conclusioni.....	343

Capitolo VIII - La diffamazione via *web* nell'epoca dei *social network*
di Francesco Pio Lasalvia

1. Premessa.....	346
2. La diffamazione come reato tradizionale commesso via <i>internet</i>	348
3. La qualificazione giuridica: il <i>web</i> è sempre “mezzo di pubblicità”?.....	356
4. La (ir)responsabilità delle figure diverse dall'autore della diffamazione	364
5. <i>Internet</i> spazio senza confini. Problemi di individuazione del <i>locus commissi delicti</i>	375
6. Tra libertà <i>del web</i> e sicurezza <i>sul web</i> . Brevi spunti di riflessione <i>de iure condendo</i>	380

Capitolo IX - La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p.
di Stefano Delsignore

1. Premessa.....	388
2. Le ragioni dell'introduzione del delitto di pornografia minorile.....	390
3. Il recepimento della “Convenzione di Lanzarote” con la L. 1.10.2012, n. 172	393
4. Collocazione sistematica e bene giuridico tutelato	395
4.1. Le non condivisibili tesi dottrinali che individuano il bene giuridico nella libertà di autodeterminazione sessuale e nella dignità umana	404
5. La natura di reati di pericolo astratto dei delitti di cui all'art. 600-ter	409
6. Le fattispecie previste dall'art. 600-ter c.p.	416
7. Soggetto attivo	417
8. Soggetto passivo	418
9. La definizione di pornografia minorile.....	421
9.1. Le elaborazioni dottrinali e giurisprudenziali che hanno preceduto la nuova definizione normativa	421
9.2. La nuova definizione normativa di pornografia minorile introdotta nel 2012.....	426

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-quater.1	434
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...	439
10.1. Il delitto di realizzazione di esibizioni o spettacoli pornografici utilizzando minori	446
10.2. Il delitto di produzione di materiale pornografico minorile	450
10.3. Il delitto di induzione o reclutamento dei minori a partecipare ad esibizioni o spettacoli pornografici	452
10.4. Il delitto di percezione di altro profitto dai suddetti spettacoli ..	454
10.5. Elemento soggettivo	455
10.6. Individuazione dei momenti consumativi e configurabilità del tentativo	456
11. Il delitto previsto dall'art. 600-ter, comma 2: commercio del materiale pedo-pornografico	458
11.1. Elemento oggettivo	458
11.2. Elemento soggettivo	460
11.3. Individuazione del momento consumativo e configurabilità del tentativo	461
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	461
12.1. Elemento oggettivo: le condotte tipiche	462
12.2. I mezzi di commissione. Il problema delle chat-line e degli <i>Internet Service Providers</i>	465
12.3. L'oggetto materiale	467
12.4. Elemento soggettivo	470
12.5. Individuazione del momento consumativo e configurabilità del tentativo	472
13. Il delitto dell'art. 600-ter, comma 4: offerta e cessione di materiale pornografico	473
13.1. Elemento oggettivo. Le condotte	474
13.2. L'oggetto materiale: «materiale pornografico di cui al primo comma»	476
13.3. Elemento soggettivo	477

13.4. Individuazione del momento consumativo e configurabilità del tentativo.....	478
14. Il “nuovo” delitto previsto dal comma 6 dell’art. 600-ter: assistere ad esibizioni o spettacoli pornografici minorili	478
14.1. Elemento soggettivo.....	480
14.2. Individuazione del momento consumativo e configurabilità del tentativo.....	480
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.....	480
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.	484
17. Concorso di norme e concorso di reati	487
18. Il raddoppio del termine prescrizione	491
19. Brevi cenni ad alcune questioni processuali	491
20. Responsabilità degli enti per la commissione dei delitti previsti dall’art. 600-ter c.p.	494

Capitolo X - 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.....	503
2. Cenni di diritto comparato	511
3. Soggetto attivo	528
4. Soggetto passivo	529
5. Elemento oggettivo. Le condotte tipizzate dall’art. 600-quater c.p.: “procurarsi” e “detenere”.....	530
5.1. Procurarsi.....	531
5.2. Detenere	532
5.3. Oggetto materiale: il materiale pornografico realizzato utilizzando minori degli anni diciotto ed il materiale di produzione “artigianale”	536
6. La rilevanza della pornografia parzialmente virtuale nell’ambito delle fattispecie previste dall’art. 600-quater c.p. (rinvio)	541
7. Elemento soggettivo. Il significato da attribuire all’avverbio consapevolmente.....	541
8. Individuazione del momento consumativo e configurabilità del tentativo	543
9. Concorso di norme e concorso di reati	544

10. La circostanza aggravante dell'ingente quantità, le aggravanti di cui all'art. 602-ter c.p., l'attenuante prevista dall'art. 600-septies.1 c.p. e i profili sanzionatori	546
11. Cenni a talune questioni processuali	550
12. Responsabilità delle persone giuridiche per la commissione delle fattispecie previste dall'art. 600-quater c.p.....	554

Capitolo XI - 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	559
2. Profili generali	563
3. Interesse tutelato	563
4. Il concetto di “virtuale”.....	567
5. Applicazione giurisprudenziale	569
6. Legittimità costituzionale e questioni interpretative aperte	573
7. Conclusioni.....	576

Capitolo XII - Sexting, minori e diritto penale

di Ivan Salvadori

1. Introduzione.....	581
2. Il concetto di <i>sexting</i>	583
3. Gli effetti negativi del <i>sexting</i> sui minori.....	584
4. <i>Sexting</i> e pedopornografia.....	585
5. Rapporti sessuali tra e con minorenni: efficacia del consenso.....	587
6. Rilevanza penale delle condotte aventi ad oggetto pornografia minorile.....	589
6.1. Produzione di pedopornografia	592
6.2. Distribuzione, divulgazione, diffusione, pubblicizzazione, offerta e cessione di pedopornografia.....	595
6.3. Detenzione di pedopornografia	599
7. Gli orientamenti giurisprudenziali in materia di <i>sexting</i>	602
8. Conclusioni.....	608

Capitolo XIII - Adescamento di minorenni

di Salvatore De Bonis

1. Premessa.....	617
2. Bene giuridico tutelato.....	619
3. Soggetto attivo e soggetto passivo	620
4. La condotta tipica	622

5. Momento consumativo e tentativo.....	624
6. Elemento soggettivo	625
7. Le previsioni circostanziali	626
8. Cenni in tema concorso di norme e di reati	627
9. Pene, altri aspetti sanzionatori e regime di procedibilità.....	628

Capitolo XIV - Il cyberstalking

di Francesco Macrì

1. Lo <i>stalking</i> quale fenomeno criminologico e la sua incidenza statistica in Italia	631
2. Il delitto di “Atti persecutori” di cui all’art. 612- <i>bis</i> c.p.....	634
3. Il <i>cyberstalking</i> in generale	637
4. Il <i>cyberstalking</i> : profili criminologici	638
5. Il <i>cyberstalking</i> : la fattispecie aggravata di cui all’art. 612- <i>bis</i> , comma 2, c.p.....	642

Capitolo XV - La diffusione di immagini sessualmente esplicite

di Paolo Beccari e Gian Marco Caletti

1. Premessa. Il fenomeno della diffusione non consensuale di immagini sessualmente esplicite. Inadeguatezza del neologismo “ <i>revenge porn</i> ”	645
2. L’esigenza di una criminalizzazione specifica tra offensività ed <i>extrema ratio</i> . Cenni al quadro giuridico preesistente	647
3. L’introduzione dell’art. 612- <i>ter</i> c.p. La struttura della norma incriminatrice e la sua collocazione sistematica	649
4. Le condotte tipizzate.....	651
5. L’oggetto della condotta: le immagini e i video tra connotazione sessuale e privacy	653
6. Il presupposto dell’assenza di consenso alla diffusione. Profili inerenti all’imputazione colpevole	655
7. Cenni al problema dei “secondi distributori”. L’eterogenesi dei fini e il dolo specifico quale criterio di imputazione dell’ipotesi base	658
8. Una prima lettura giurisprudenziale dell’art. 612- <i>ter</i> : difficoltà applicative della privacy e “resistenze” del neologismo “ <i>revenge porn</i> ”	661
9. Il “vuoto di tutela” sulla creazione non consensuale di materiali sessualmente espliciti: un antifatto punibile per analogia?.....	663

Capitolo XVI - Il cyberbullismo

di Maria Chiara Parmiggiani

1. Premessa.....	669
------------------	-----

2. <i>Ratio</i> della legge.....	672
3. La definizione di cyberbullismo	673
4. Elemento oggettivo	674
4.1. La molestia, l'ingiuria e la diffamazione	675
4.2. Il ricatto	676
4.3. Il furto d'identità.....	677
4.4. L'alterazione, l'acquisizione illecita e la manipolazione di dati personali	678
4.5. Il trattamento illecito di dati personali.....	678
4.6. La pressione, l'aggressione, la denigrazione e la diffusione di contenuti <i>online</i>	679
5. Elemento soggettivo	679
6. Gli effetti del cyberbullismo.....	680
7. La tutela della persona offesa	681
8. Gli strumenti preventivi	684
9. Gli strumenti di tipo ripristinatorio e cautelare	685
10. Riflessioni (provvisoriamente) conclusive	687

Capitolo XVII - I reati contro la riservatezza informatica

di Ivan Salvadori

1. Premessa sistematica	694
2. Delimitazione dell'ambito della trattazione	696
3. La riservatezza informatica	698
4. L'interrelazione tra riservatezza informatica e sicurezza informatica	702
5. Accesso abusivo ad un sistema informatico o telematico (art. 615- <i>ter</i> c.p.).....	704
5.1. La condotta tipica	704
5.2. L'abusività delle condotte di introduzione e di permanenza in un sistema informatico o telematico	707
5.2.1. L'abusività come perseguimento di finalità contrarie a quelle per le quali l'autorizzazione all'accesso è stata concessa.....	710
5.2.2. L'abusività quale violazione delle disposizioni che disciplinano l'introduzione o il mantenimento in un sistema informatico.....	712
5.3. La nozione di misure di sicurezza.....	714
5.4. L'elemento soggettivo	715
5.5. Momento consumativo e tentativo.....	716
5.6. Circostanze aggravanti	717

5.6.1.	L'accesso abusivo commesso da un funzionario pubblico con abuso di poteri o violazione dei doveri o da un investigatore privato	717
5.6.2.	L'abuso della qualità di operatore di sistema.....	723
5.6.3.	L'accesso abusivo commesso con violenza sulle cose, alle persone o da parte di chi è palesemente armato	723
5.6.4.	Il danneggiamento di dati o di sistemi informatici susseguente all'accesso abusivo	724
5.6.5.	L'accesso abusivo a sistemi informatici o telematici di "interesse pubblico"	725
5.7.	Struttura del reato e bene giuridico tutelato	726
6.	Detenzione, diffusione ed installazione abusive di apparecchiature, codici ed altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615- <i>quater</i> c.p.).....	729
6.1.	La condotta tipica	730
6.2.	L'abusività della condotta	732
6.3.	L'oggetto materiale del reato.....	734
6.4.	L'elemento soggettivo	735
6.5.	Momento consumativo e tentativo	736
6.6.	Circostanze aggravanti	737
6.7.	Struttura del reato e bene giuridico tutelato	737
7.	Detenzione, diffusione ed installazione abusive di apparecchiature, dispositivi o <i>software</i> diretti a danneggiare un sistema informatico o telematico (art. 615- <i>quinquies</i> c.p.).....	738
7.1.	La condotta tipica	739
7.2.	L'oggetto materiale del reato.....	740
7.3.	L'elemento soggettivo	741
7.4.	Momento consumativo e tentativo	741
8.	Le intercettazioni informatiche e telematiche	741
8.1.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617- <i>quater</i> c.p.)	743
8.1.1.	La condotta tipica	743
8.1.2.	L'oggetto materiale del reato	746
8.1.3.	L'elemento soggettivo.....	747
8.1.4.	Momento consumativo e tentativo	747
8.1.5.	Circostanze aggravanti.....	747
8.1.6.	Struttura del reato e bene giuridico tutelato	749
8.2.	Detenzione, diffusione e installazioni abusive di apparecchiature e di altri mezzi atti ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617- <i>quinquies</i> c.p.).....	749

8.2.1. La condotta tipica	750
8.2.2. L'oggetto materiale	752
8.2.3. L'elemento soggettivo	752
8.2.4. Momento consumativo e tentativo	753
8.2.5. Circostanze aggravanti	753
8.2.6. Struttura del reato e bene giuridico tutelato	753
8.3. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617- <i>sexies</i> c.p.) ..	754
8.3.1. La condotta tipica	754
8.3.2. L'oggetto materiale del reato	755
8.3.3. L'elemento soggettivo	756
8.3.4. Momento consumativo e tentativo	756
8.3.5. Circostanze aggravanti	756
8.3.6. Struttura del reato e bene giuridico tutelato	757
9. La nozione di «corrispondenza» informatica o telematica	757

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	764
2. L'estorsione <i>on line</i>	767
3. <i>Sex torsion</i> via <i>web</i> ed estorsione a mezzo <i>Ransomware</i>	768
4. Bene giuridico	773
5. Soggetto attivo e soggetto passivo	774
6. Elemento materiale	775
6.1. La condotta violenta	776
6.2. La condotta minacciosa	778
6.3. Lo stato di coazione del soggetto passivo	780
6.4. L'atto di disposizione patrimoniale coartato	782
6.5. L'ingiusto profitto ed il danno altrui	782
7. Elemento soggettivo	784
8. Consumazione e tentativo	785
9. Profili sanzionatori e circostanze aggravanti	789
10. Rapporto delle cyber-estorsioni con altri reati	791
10.1. Estorsione informatica ed esercizio arbitrario delle proprie ragioni	791
10.2. Il rapporto con la violenza privata	793
10.3. <i>Sex-torsion</i> via <i>web</i> e violenza sessuale	794
10.4. <i>Sex-torsion</i> via <i>web</i> e reati di pedopornografia	796

10.5. Estorsione a mezzo <i>Ransomware</i> ed art. 615- <i>quinquies</i> c.p.....	798
10.6. Estorsione a mezzo <i>Ransomware</i> e danneggiamento informatico	801
10.7. Estorsione a mezzo <i>Ransomware</i> e accesso abusivo a sistema informatico o telematico	803

Capitolo XIX - I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici

di Alberto Cappellini

1. Introduzione.....	810
2. Evoluzione e quadro della normativa.....	815
2.1. La riforma del 1993	816
2.2. Gli impulsi internazionali e la riforma del 2008.....	819
2.3. Gli interventi operati dal D.Lgs. 15.1.2016, n. 7, in tema di depenalizzazioni, e dalla L. 23.12.2021, n. 238, circa il delitto di cui all'art. 615- <i>quinquies</i> c.p.	823
3. I delitti di danneggiamento di dati e sistemi "privati" (artt. 635- <i>bis</i> e 635- <i>quater</i> c.p.).....	824
3.1. Il soggetto attivo	825
3.2. Gli oggetti materiali	825
3.3. Le condotte	831
3.4. Gli eventi	836
3.5. L'elemento soggettivo	840
3.6. La consumazione e il tentativo	841
3.7. Le circostanze aggravanti specifiche.....	841
3.8. Rapporti tra reati.....	843
3.9. Profili sanzionatori e processuali. La responsabilità degli enti.	845
4. I delitti di danneggiamento di dati e sistemi "pubblici" (artt. 635- <i>ter</i> e 635- <i>quinquies</i> c.p.).....	847
4.1. Il soggetto attivo	848
4.2. Gli oggetti materiali	848
4.3. Le condotte	850
4.4. L'elemento soggettivo	852
4.5. La consumazione e il tentativo	853
4.6. Gli eventi aggravatori.....	853
4.7. Le circostanze aggravanti specifiche.....	854
4.8. Rapporti tra reati.....	855
4.9. Profili sanzionatori e processuali. La responsabilità degli enti.	856
5. Il delitto di diffusione di apparecchiature, dispositivi o programmi nocivi (art. 615- <i>quinquies</i> c.p.)	857

5.1.	Il soggetto attivo	858
5.2.	Gli oggetti materiali	858
5.3.	Le condotte	861
5.4.	L'elemento soggettivo	863
5.5.	La consumazione e il tentativo	865
5.6.	Rapporti tra reati.....	865
5.7.	Profili sanzionatori e processuali. La responsabilità degli enti.	867
6.	L'equiparazione della "violenza informatica" alla violenza sulle cose (art. 392, ultimo comma, c.p.)	867

Capitolo XX - I dati informatici come "cosa mobile" oggetto di furto o appropriazione indebita

di Clementina Colucci

1.	Premessa.....	877
2.	Il concetto di "cosa mobile" nel diritto penale	878
3.	L'estensione del concetto di "cosa mobile" ai dati informatici: fisicità, materialità, mobilità.....	881
4.	Le condotte "aggressive" del dato informatico: trasferimento, copia, captazione intellettuale	885
5.	Possibili soluzioni <i>de iure condito</i> e <i>de iure condendo</i>	889

Capitolo XXI - Le frodi informatiche

di Gherardo Minicucci

1.	Il delitto di frode informatica (art. 640-ter c.p.)	893
1.1.	Il soggetto attivo	896
1.2.	La condotta	896
1.3.	Gli eventi	902
1.4.	L'elemento soggettivo	902
1.5.	La consumazione e il tentativo	903
1.6.	Le circostanze aggravanti speciali	903
1.7.	La truffa sul <i>web</i>	906
1.8.	Il <i>phishing</i>	907
1.9.	Rapporti tra reati.....	909
1.10.	Profili sanzionatori e processuali. Le confische	912
2.	Il delitto di frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)	915
2.1.	Il soggetto attivo	916
2.2.	La condotta	916
2.3.	L'elemento soggettivo	918
2.4.	La consumazione e il tentativo	919

2.5. Rapporti tra reati.....	920
2.6. Profili sanzionatori e processuali. La confisca	920

Capitolo XXII - Il cybericiclaggio

di Vito Plantamura

1. Il riciclaggio e il reimpiego	925
1.1. L'autoriciclaggio.....	932
2. Il cybericiclaggio.....	941
3. Il cybericiclaggio e la criminalità organizzata	944
3.1. In particolare: il finanziamento del terrorismo	947
4. Il cybericiclaggio e le valute virtuali	950
5. Il cybericiclaggio e il <i>gambling online</i>	954
6. Conclusioni.....	955

Capitolo XXIII - 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	962
2. Il delitto di trattamento illecito di dati personali (art. 167 Cod. <i>privacy</i>)	965
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 Google-Vivi Down	968
2.2. (Segue) Ulteriore sviluppo della giurisprudenza della Cassazione in materia di responsabilità penale dell' <i>internet provider</i> : pregi e limiti	976
3. Il reato contravvenzionale di omessa adozione di misure minime di sicurezza nei trattamenti elettronici di dati personali (art. 169 Cod. <i>privacy</i>).....	982
4. I reati contro il diritto alla <i>privacy</i> "informatica" del lavoratore: l'art. 171 Cod. <i>Privacy</i>	986
4.1. (Segue) ... e i reati del Codice penale a tutela delle comunicazioni informatiche.....	992
5. Le novità apportate dal GDPR e il D.Lgs. 18.5.2018, n. 51 recante attuazione della Direttiva 2016/680/UE sul trattamento dei dati personali in ambito penale.....	996

Capitolo XXIV - 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.....	1002
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)	1005
3. Le sanzioni amministrative (art. 162- <i>ter</i> , D.Lgs. 30.6.2003, n. 196)	1012
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>).....	1013
5. Gli obblighi in caso di <i>data breach</i> nel Reg. 2016/679/UE sulla protezione dei dati personali	1022
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	1026

Capitolo XXV - Il sistema delle tutele nel Regolamento europeo n. 679/2016 sulla protezione dei dati personali

di Daniele Labianca

1. Introduzione.....	1035
2. Il Regolamento <i>privacy</i> europeo del 2016. Genesi e precedenti.....	1037
3. (Segue) La struttura del Regolamento. I diritti dell'interessato	1040
4. I mezzi di tutela dell'interessato	1050
4.1. (Segue) Il ricorso in via amministrativa all'autorità di controllo (art. 77)	1051
4.2. (Segue) Il ricorso avverso un provvedimento dell'autorità (art. 78).....	1052
4.3. (Segue) L'impugnazione delle decisioni del Comitato europeo per la protezione dei dati	1054
4.4. (Segue) La tutela giurisdizionale nei confronti del titolare del trattamento o del responsabile del trattamento	1054
5. La tutela risarcitoria.....	1055
6. L'apparato sanzionatorio amministrativo	1058
7. La facoltà per gli Stati membri di adottare "altre" sanzioni. Le sanzioni penali ed il principio del <i>ne bis in idem</i>	1062
8. L'interferenza della disciplina eurounitaria con la normativa italiana. L'adeguamento dell'ordinamento interno: il D.Lgs. n. 101/2018. Cenni e rinvio	1067

Capitolo XXVI - I reati in materia di protezione dei dati personali*di Federica Resta*

1. I reati previsti dal D.Lgs. n. 51/2018.....	1076
1.1. Profili generali.....	1076
1.2. Le fattispecie di reato	1080
1.2.1. Trattamento illecito.....	1080
1.2.2. Falsità in atti e dichiarazioni al Garante.....	1081
1.2.3. Inosservanza di provvedimenti del Garante	1082
1.2.4. Gli illeciti commessi nel contesto dell'intelligence	1083
2. I reati previsti dal D.Lgs. n. 196/2003, come novellato dal D.Lgs. n. 101/2018.....	1084
2.1. Profili generali.....	1084
2.2. Le fattispecie di reato	1089
2.2.1. Trattamento illecito di dati.....	1089
2.2.2. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala	1091
2.2.3. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	1094
2.2.4. Disposizioni ulteriori	1095

Capitolo XXVII - La tutela penale dei diritti d'autore e connessi*di Roberto Flor*

1. Premessa.....	1100
2. Percorsi storici	1103
3. Le più recenti fonti internazionali ed europee (cenni)	1110
4. La tutela penale dei diritti d'autore in Italia.....	1114
5. I "caratteri generali" del sistema di tutela penale del diritto d'autore e dei diritti connessi	1116
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.....	1130
7. Le principali fattispecie penali previste dalla l.d.a.....	1146
7.1. Art. 171 l.d.a.	1147
7.2. Art. 171-bis l.d.a.	1149
7.2.1. La duplicazione abusiva di un programma per elaboratore	1153
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	1160

7.2.3. La tutela penale delle banche dati	1172
7.3. Art. 171-ter l.d.a.	1180
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	1182
7.3.2. I più recenti e frequenti casi di applicazione dell’art. 171-ter l.d.a.	1189
7.4. Tutela penale e autotutela tecnologica dei diritti d’autore	1192
8. Gli artt. 171-ter, 171-octies e 174-bis l.d.a. e le questioni di costituzionalità	1199
9. L’art. 171-octies.1 e l’art. 171-nonies l.d.a.	1203
10. La responsabilità dell’ <i>Internet Service Provider</i> per le violazioni penali dei diritti d’autore (cenni): uno sguardo tra passato, presente e futuro... ..	1205
11. Beni giuridici protetti e progresso culturale, sociale ed economico	1217
12. Le “tendenze” europee: il ruolo propulsore della Corte di Giustizia e l’evoluzione delle tutele dei diritti d’autore (cenni).....	1221

Parte III

Diritto penale sostanziale: nuove frontiere

Capitolo I - Il problema della responsabilità per l’uso di intelligenze artificiali

di Maria Beatrice Magro

1. Le caratteristiche delle Intelligenze Artificiali evolute	1232
2. I campi di applicazione delle Intelligenze Artificiali	1235
3. A favore di una proficua complementarietà tra umani e macchine	1237
4. Intelligenza Artificiale “forte” e “debole”	1237
5. Intelligenza, razionalità e senso comune	1241
6. Le emozioni artificiali dei robot	1243
7. Questioni di “roboetica”: l’agire conforme a regole delle Intelligenze Artificiali	1244
8. I robot intelligenti: oggetti o soggetti giuridici?	1246
9. Le Intelligenze artificiali possono essere responsabili penalmente per il loro agire?.....	1247
10. La responsabilità dolosa per l’uso di Intelligenze Artificiali	1250
11. La responsabilità colposa per l’uso di Intelligenze Artificiali.....	1251
12. I rischi dell’innovazione tecnologica	1254

Capitolo II - Potenziamento cognitivo e diritto penale*di Letizia d'Altilia*

1. Il potenziamento umano: profili generali.....	1257
2. Il potenziamento cognitivo “farmacologico”	1261
2.1. Il dato statistico	1263
2.2. Le questioni aperte.....	1266
3. I riflessi sul piano penalistico	1268
3.1. Per un’eventuale regolamentazione del fenomeno: modelli e limiti.....	1269
3.2. Un “nuovo” concetto di salute.....	1271
3.3. Un “nuovo” concetto di malattia e le conseguenze in tema di lesioni personali.....	1274
3.4. Il ruolo “chiave” del consenso informato	1276
3.5. La prescrizione di farmaci <i>off label</i> e la responsabilità del medico	1280
4. La medicina potenziativa nel Codice di deontologia medica	1282
5. Qualche nota conclusiva	1284

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 “ <i>post-verità</i> ”	1290
2. I tentativi di regolamentazione normativa in Italia: “ <i>fake news</i> ” o “ <i>fake laws</i> ”?.....	1293
2.1. Il percorso ricostruttivo dei principali disegni di legge per il contrasto alle <i>fake news</i> : dal c.d. “d.d.l. Gambaro”.....	1294
2.2. ... al progetto Zanda-Filippin e l’influente impatto della “soluzione tedesca”.....	1299
3. La fugace esperienza del modello “ <i>red button</i> ” all’italiana.....	1304
4. Le ultime pagine di una storia ancora tutta da scrivere: l’Unità di monitoraggio per il contrasto della diffusione di <i>fake news</i> relative al COVID-19 ed i più recenti sviluppi in ambito comunitario	1305

Capitolo IV - Il *cyberwarfare*: gli scenari della guerra informatica*di Mario L'Insalata*

1. Informatica e minacce dell'Era moderna.....	1310
2. Definizione di " <i>cyberwarfare</i> "	1314
2.1. Tipi di <i>cyberwarfare</i>	1316
2.2. Finalità della <i>cyberwarfare</i>	1317
2.3. Modalità attuative	1319
2.3.1. Spionaggio	1319
2.3.2. Sabotaggio	1320
2.3.3. Guerra psicologica.....	1322
2.3.4. Dissuasione	1323
2.4. Pubblicità o segretezza degli atti di <i>cyberwarfare</i>	1323
2.5. <i>Cyberdefence</i>	1324
3. Modalità operative di <i>cyberwarfare</i> e loro riconducibilità a fattispecie dell'ordinamento penale italiano	1325
4. La giurisdizione sulle condotte di <i>cyberwarfare</i>	1331
5. La normativa italiana ed europea per la difesa dagli attacchi informatici.....	1332

Capitolo V - Monete virtuali e diritto penale*di Ranieri Razzante*

1. L'impiego delle valute virtuali per fini illeciti e identikit del <i>cyber-criminale</i>	1337
2. Il fenomeno del <i>cyberlaundering</i> : il lavaggio di denaro sporco approda in rete	1342
3. Prevenire e combattere il riciclaggio con le valute virtuali. Aspetti normativi	1345
4. I recenti sviluppi della giurisprudenza penale in tema di riciclaggio, autoriciclaggio e valute virtuali.....	1348

Capitolo VI - La responsabilità penale dell'intelligenza artificiale: i termini generali del problema, con particolare riguardo alle auto senza conducente*di Patrizia Giusti*

1. Introduzione.....	1356
2. I veicoli autonomi: definizione e classificazione.....	1356
2.1. Il funzionamento di un veicolo a guida autonoma	1359
2.2. ADAS: i sistemi avanzati di assistenza alla guida	1360
2.3. Solo macchine od anche personalità giuridica?.....	1361
3. Una prima disciplina: la frammentaria normativa americana.....	1362

3.1. Il caso <i>Autopilot</i> di Tesla	1365
4. La normativa dell'Unione Europea.....	1367
5. Il diritto italiano	1368
5.1. In particolare, la responsabilità da prodotto	1374
5.2. La responsabilità per rischio di impresa	1374
6. Gli altri ordinamenti europei	1375
6.1. L'esperienza anglosassone	1376
6.2. L'esperienza francese	1376
6.3. L'esperienza tedesca.....	1376
7. Conclusioni.....	1377

Capitolo VII - La responsabilità penale per le auto a guida autonoma
di Massimiliano Lanzi

1. Attualità e prospettive in tema di intelligenza artificiale <i>embodied e self-driving cars</i>	1379
2. La cornice normativa della mobilità autonoma	1382
3. Veicoli autonomi come strumento del reato.....	1383
4. <i>Autonomous Vehicles</i> e colpa stradale.....	1385
4.1. La posizione di garanzia del conducente di <i>self-driving cars</i> ...	1385
4.2. Veicoli autonomi e responsabilità penale da prodotto difettoso	1387

Capitolo VIII - L'intelligenza artificiale come vittima del reato
di Costanza Corridori

Sezione I - La personalità giuridica dell'intelligenza artificiale

1. La personalità elettronica	1394
2. Il libero arbitrio dell'intelligenza artificiale	1396

Sezione II - Intelligenza artificiale come vittima del reato

1. Macchine intelligenti vittime di reato.....	1397
2. Delitti contro la persona "robotica"	1398

Capitolo IX - Intelligenza artificiale e abusi di mercato
di Giandomenico Salcuni e Mattia Di Florio

1. Una premessa ricostruttiva.....	1403
2. Algoritmi e diritto penale: brevi cenni	1406
2.1. Opacità degli algoritmi	1408
3. L'abuso penalmente rilevante di informazioni privilegiate	1412
4. La fattispecie penale di manipolazione del mercato	1414
5. Conclusioni.....	1416

Capitolo X - La responsabilità penale del sanitario alla luce dell'evoluzione tecnologica

di *Valentina Badalamenti*

1. Premessa: la trasformazione della Salute.....	1423
2. I rischi e i benefici della medicina presente e futura.....	1425
2.1. La tutela della libertà terapeutica e di autodeterminazione nell'ambito del rapporto medico-paziente	1427
2.2. Il regime di responsabilità applicabile all'errore della macchina	1429
3. Alcune considerazioni conclusive.....	1433

Capitolo XI - Responsabilità da reato degli enti e intelligenza artificiale

di *Alice Giannini*

1. Premesse.....	1437
2. I modelli di responsabilità penale dell'ente	1438
3. L'analogia fra IA e persone giuridiche	1441
4. La configurabilità di una responsabilità dell'ente per l'agire algoritmico	1445
5. Conclusioni.....	1449

Capitolo XII - L'impatto del *deepfake* sul diritto penale

di *Margherita Piccardi*

1. Il fenomeno del <i>deepfake</i> . Tra furto d'identità e violazione della <i>privacy</i>	1453
2. Gli interventi del Garante per la tutela dei dati personali.....	1455
3. Le disposizioni vigenti in materia di contrasto al fenomeno nel nostro ordinamento giuridico.....	1457
3.1. <i>De iure condendo</i>	1459
4. Il <i>porno-deepfake</i> o <i>deepnude</i>	1462
4.1. <i>De lege ferenda</i>	1466
5. Conclusioni.....	1467

Capitolo XIII - I reati nel metaverso

di *Nicolò Bussolati*

1. Il metaverso	1469
2. L'interazione	1471
3. I dati, i beni e la valuta virtuale.....	1472
4. Il contenuto e la rappresentazione.....	1475
5. Il sé virtuale e la sua espressione	1477

Capitolo XIV - Intelligenza artificiale e legislazione penale

di Michele Papa e Giulia Tavella

1. Una incerta visione del futuro	1483
2. Dal diritto come “testo” al diritto come “code”	1486
3. Intelligenza artificiale e rinnovamento della fattispecie incriminatrice ..	1491
4. Intelligenza artificiale e nuova organizzazione della legislazione penale: dal codice ai <i>networks</i> e alle <i>playlists</i> di norme.....	1494

Parte IV

Diritto processuale penale

Capitolo I - Le prove informatiche

di Giorgio Spangher

1. Lo sfondo	1501
2. La prova	1501
3. Le regole.....	1502

Capitolo II - L'evoluzione delle categorie tradizionali: il documento informatico

di Paolo Tonini

1. Il documento informatico: categorie civilistiche e penalistiche.....	1506
2. L'informatica come presunta forma di rappresentazione di un fatto	1507
3. L'informatica come forma di incorporamento della rappresentazione di un fatto	1509
4. Il documento informatico tra immaterialità e dematerializzazione	1510
5. La definizione di documento informatico.....	1511
6. Documento informatico e contraddittorio.....	1514
7. L'estrazione della copia di un <i>file</i> dal <i>computer</i>	1514
8. La non ripetibilità nell'informatica forense	1517
9. La correlazione tra la definizione di documento informatico e la forma di acquisizione del medesimo.....	1517
10. Considerazioni sul concetto di non ripetibilità.....	1518
11. Non ripetibilità e riforma dell'art. 111 Cost.	1519
12. Non ripetibilità e nucleo insopprimibile del contraddittorio.....	1522
13. La tutela del contraddittorio <i>ex post</i>	1523

Capitolo III - La prova informatica e il mancato rispetto delle *best practices*: lineamenti sistematici sulle conseguenze processuali

di Carlotta Conti

1. Nuovi paradigmi	1527
2. L'insufficienza del contraddittorio contestuale o postumo	1529
3. <i>Forma essentialis</i> e inutilizzabilità tra <i>an</i> e <i>quomodo</i>	1533
4. Tre modelli di eterointegrazione dei divieti	1537
5. La ricostruzione in punto di regole di valutazione.....	1542
6. L'onere della prova.....	1544
7. Considerazioni conclusive	1547

Capitolo IV - La Convenzione di Budapest del 2001 e la L. n. 48/2008

di Stefano Aterno

1. Premessa.....	1551
2. La L. n. 48/2008 in generale e alcuni aspetti tecnico giuridici fondamentali	1554
3. L'accertamento tecnico urgente sui supporti informatici	1564
4. La custodia delle cose sequestrate <i>ex art. 259 c.p.p.</i>	1566
5. Il sequestro di corrispondenza inoltrata per via telematica <i>ex art. 254 c.p.p.</i>	1568
6. Atti ripetibili e atti irripetibili	1572
7. Il Secondo Protocollo aggiuntivo alla Convenzione di Budapest sulla cooperazione rafforzata e la divulgazione delle prove elettroniche.....	1575

Capitolo V - Le ispezioni e perquisizioni di dati e sistemi

di Paola Felicioni

1. Ispezioni e perquisizioni tra evoluzione tecnologica ed evoluzione normativa.....	1583
2. Ispezione informatica e perquisizione informatica: profili definitivi	1587
2.1. La nozione	1588
2.2. L'oggetto della ricerca ispettiva e perquirente.....	1593
2.3. L'oggetto investito dalla ricerca probatoria: sistemi informatici o telematici	1596
2.4. Il labile discrimine tra ispezione informatica e perquisizione informatica.....	1600
2.5. La copia forense come tecnica di ricerca o accertamento autonomo: rinvio.....	1604
3. Ricerca della prova informatica e diritti fondamentali.....	1605
3.1. I diritti dell'individuo	1606

3.2.	I diritti processuali	1609
4.	La dinamica probatoria: ricognizione normativa e profili di specialità ..	1613
4.1.	La motivazione del provvedimento.....	1613
4.2.	Le procedure di <i>computer forensics</i> : individuazione del reperto, acquisizione e analisi dei dati digitali	1617
4.3.	Le modalità esecutive.....	1628
4.4.	L'esame di dati, informazioni e programmi informatici presso banche	1633
4.5.	Le garanzie difensive	1634

Capitolo VI - Il sequestro di dati e sistemi

di Alessandra Testaguzza

1.	Il valore della prova informatica nel processo penale.....	1643
2.	La Convenzione di Budapest e i nuovi mezzi di ricerca della prova.....	1645
3.	Le <i>best practices</i> nelle indagini informatiche	1647
4.	Il sequestro probatorio di dati e sistemi informatici.....	1652
5.	La dubbia natura giuridica dei sequestri di dati e sistemi.....	1657
6.	Aspetti problematici	1659
7.	Il sequestro di siti <i>web</i> e delle testate giornalistiche <i>online</i>	1664

Capitolo VII - Accertamento tecnico ripetibile. La gestione del reperto informatico

di Vincenzo Lagi

1.	Introduzione.....	1671
2.	Il dato informatico	1673
3.	Le fasi dell'accertamento	1675
4.	Ripetibilità e <i>best practices</i>	1678
5.	Conclusioni.....	1680

Capitolo VIII - Il captatore informatico, fra tipicità e atipicità probatoria

di Marco Torre

1.	Il captatore informatico: un problema di “tassonomia” probatoria	1684
2.	Captatore informatico e intercettazioni: necessità di una <i>actio finium regundorum</i>	1687
2.1.	Le intercettazioni telefoniche	1687
2.2.	Le intercettazioni telematiche	1690
2.3.	Le intercettazioni di conversazioni tra presenti	1691
2.3.1.	Limiti di ammissibilità	1692
2.3.2.	Presupposti e forme del provvedimento di autorizzazio-	

ne	1694
2.3.3. Esecuzione delle operazioni e verbalizzazione delle intercettazioni.....	1696
2.3.4. Regime di utilizzabilità	1698
3. La poliedricità del captatore informatico: atipicità vs legalità processuale.....	1699
3.1. Le c.d. perquisizioni on line.....	1699
3.2. I <i>keylogger software</i> : cenni.....	1701
3.3. Le videoriprese investigative: cenni.....	1702
4. Conclusioni.....	1703

Capitolo IX - Open source intelligence: spionaggio digitale e social network
di Marco Torre

1. <i>Open source intelligence</i> : definizione e classificazioni	1708
2. <i>Open Source Intelligence</i> e indagini penali	1710
3. SOCIal Media INTelligence	1713
4. SOCMINT e dati “ristretti”: l’acquisizione mediante “inganno”	1716
5. La raccolta di dati “privati”, tra <i>voluntary disclosure</i> e <i>jurisdiction to investigate</i> : il Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche.....	1718
5.1. Le informazioni relative alla registrazione dei nomi di domicilio	1721
5.2. I subscriber data: la c.d. collaborazione diretta	1723
5.3. Le informazioni relative agli abbonati e al traffico: la cooperazione fra autorità.....	1726
5.4. La cooperazione rafforzata nelle situazioni di emergenza	1728

Capitolo X - Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema. Il sistema automatico di riconoscimento immagini
di Marco Torre

1. Intelligenza artificiale e scienze giuridiche: definizione e classificazioni.....	1731
2. Giustizia predittiva: cenni	1737
3. Intelligenza artificiale e indagini penali.....	1742
4. I <i>software</i> di riconoscimento di immagini	1744
5. L’esperienza italiana: Sistema Automatico di Riconoscimento Immagini (S.A.R.I.) e <i>privacy</i>	1750

Capitolo XI - Intelligenza artificiale e processo penale*di Lorenzo Algeri*

1. Intelligenza artificiale e procedimento penale: ambiti di applicazione...	1758
2. Alla ricerca di una definizione di Intelligenza artificiale	1759
3. Dai neuroni alle reti neurali artificiali	1761
4. Intelligenza artificiale, <i>Machine learning</i> e <i>Deep learning</i>	1764
5. I <i>software</i> di “polizia predittiva”	1766
6. Intelligenza artificiale e processo penale: le certezze del modello matematico-computazionale e le incertezze del c.d. <i>automation bias</i>	1770

Capitolo XII - La competenza della procura distrettuale per i reati informatici*di Francesco Cajani*

1. Premessa: i lavori parlamentari della L. 18.3.2008, n. 48	1781
2. Il testo della Convenzione di Budapest in punto di giurisdizione e l'assenza di alcune indicazioni in materia di competenza	1783
3. I reati rientranti nella competenza c.d. distrettuale	1784
4. Regime intertemporale	1785
5. La <i>vis attractiva</i> dei procedimenti relativi ai reati c.d. distrettuali rispetto ai procedimenti relativi ad altri reati ad esso connessi	1786
6. Alcune osservazioni critiche sulla previsione di una competenza territoriale distrettuale per i <i>computer crimes</i>	1787

Capitolo XIII - Le indagini informatiche per i reati di cyberterrorismo*di Francesco Cajani*

1. Preambolo	1792
2. L'evoluzione della normativa in materia di terrorismo e l'ascesa delle nuove tecnologie	1793
3. La nozione di <i>cyberterrorismo</i>	1794
3.1. (Segue) L'ambito di applicazione delle normative in materia di cybercrime e terrorismo	1798
4. L'eterno problema della <i>data retention</i> e i rapporti con gli <i>Internet Service Provider</i>	1799
5. Il terror(ismo) che si propaga al ritmo dell' <i>instant messaging</i>	1806
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 instant messaging) con protocolli di crittografia e delle caselle di posta elettronica @.com	1810

6. Il monitoraggio della Rete e il tempestivo intervento di rimozione di contenuti illeciti <i>online</i>	1815
7. Casi di accessi transfrontalieri a dati informatici: una prospettiva legale.....	1817
8. Quali previsioni per un futuro ancora incerto?.....	1820

Capitolo XIV - 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	1825
2. I reati di pedopornografia <i>online</i> e le indagini informatiche: tra comode astrattezze e bisognose concretezze	1828
3. Le attività di contrasto “digitali” <i>ex art. 14, L. n. 269/1998</i>	1832
4. Il rispetto dei limiti normativi quale <i>condicio sine qua non</i> per la legittimità delle operazioni <i>under cover</i>	1837
5. Utilizzabilità o non utilizzabilità del materiale probatorio? Questo è il dilemma.....	1840
5.1. Le attività di contrasto nell’ambito europeo: utili spunti di riflessione.....	1843
6. Conclusione: la necessità di un intervento legislativo come argine agli abusi degli strumenti processuali	1845

Capitolo XV - L’istituto della *data retention* tra legalità interna ed internazionale
di Stefano Marcolini

1. La descrizione tecnica del fenomeno e le libertà fondamentali incise....	1849
2. L’attuale disciplina di diritto interno: l’art. 132 Codice <i>privacy</i> tra conservazione, acquisizione ed utilizzazione	1852
3. Lo “tsunami” comunitario	1857
4. ... e le reazioni interne. Prospettive	1860

Capitolo XVI - Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati
di Gian Marco Baccari

1. Premesse.....	1868
2. La <i>data retention</i> nel codice della <i>privacy</i> del 2003	1871
3. La dichiarazione di invalidità della Dir. 2006/24 da parte della Corte di Giustizia europea.....	1873
4. Il periodo di conservazione dei dati: dalle origini ai “giorni nostri”	1875

5. (Segue) la disciplina italiana della <i>data retention</i> dopo le misure antiterrorismo del 2015 e del 2017	1877
6. Le recenti novità procedurali	1878
7. Le principali novità del D.Lgs. n. 51/2018 di attuazione della Dir. 2016/680/UE.....	1881
8. Il Regolamento sul trattamento dei dati personali da parte delle forze di polizia.....	1884

Capitolo XVII - La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche

di Marcello Daniele, aggiornamento di Silvia Signorato

1. Dalla rogatoria all'ordine europeo di indagine penale	1892
2. La raccolta delle prove digitali <i>in loco</i>	1892
2.1. L'emissione della richiesta di raccolta della prova	1893
2.2. Il rifiuto	1894
2.3. L'esecuzione.....	1897
2.4. L'utilizzabilità della prova	1900
3. La raccolta delle prove digitali a distanza.....	1902
3.1. L'acquisizione diretta di dati non riservati.....	1902
3.2. L'acquisizione diretta di dati riservati	1903
3.3. Le intercettazioni informatiche transnazionali	1905
3.4. La cooperazione transnazionale diretta con i prestatori di servizi di hosting e con i fornitori di servizi.....	1906

Capitolo XVIII - 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.....	1909
2. Il quadro giuridico dell'Unione europea in materia di cooperazione giudiziaria penale per lo scambio delle prove digitali	1911
3. Le iniziative operative delle Istituzioni europee.....	1917
4. Spunti per la realizzazione di un quadro comune europeo in materia di scambio delle prove digitali	1921
5. Scambio di prove digitali: una proposta di standard.....	1923
6. Conclusioni e prospettive future	1925

Capitolo XIX - Sistema informativo per la ricerca e la correlazione di dati investigativi basato su uno *standard* per la rappresentazione degli elementi di prova digitali

di Gerardo Giardiello e Fabrizio Turchi

1. Introduzione.....	1930
2. Lo standard di rappresentazione	1932
3. Obiettivi dello standard.....	1933
3.1. Benefici derivanti dall'uso dello standard UCO/CASE.....	1934
3.2. Gli oggetti rappresentabili tramite lo standard UCO/CASE	1935
3.3. Serializzazione di UCO/CASE.....	1938
3.4. Processo di standardizzazione	1939
4. Esempi di correlazioni investigative	1941
4.1. Accertare se un certo file è stato scambiato durante una qualsiasi comunicazione fra due sospettati, basandosi sul valore hash del file.....	1941
4.2. Accertare se un sospettato abbia visitato siti a contenuto pedo-pornografico	1944
5. Conclusioni.....	1945

Capitolo XX - *Cloud forensics*: aspetti giuridici e tecnici

di Stefano Aterno

1. Definizione teorica ed implementazioni reali dei <i>Cloud system</i>	1949
1.1. Struttura e tipi di servizi <i>Cloud</i>	1953
1.2. Sopralluogo e repertamento sui <i>Cloud</i>	1955
2. Quali norme e garanzie in tema di ispezione, perquisizione e sequestro in ambiente <i>Cloud computing</i> ?.....	1957
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>	1962
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>	1963

Capitolo XXI - *Deep web*, *dark web* e indagini informatiche. Una sintesi introduttiva

di Vincenzo Lagi

1. Introduzione.....	1969
2. L'ambito del <i>deep web</i>	1970
3. Il sottoinsieme del <i>dark web</i>	1972
4. Possibili tecniche investigative.....	1973

5. Conclusioni.....	1973
---------------------	------

Capitolo XXII - Profili penali, sostanziali e processuali, del nuovo delitto di invasione di terreni o edifici

di Luca Della Ragione e Pierluigi Zarra

1. La genesi normativa del delitto di “raduni pericolosi”.....	1976
1.1. Premessa.....	1976
2. L’inserimento provvisorio dell’art. 434- <i>bis</i> c.p. e la sua portata precettiva.....	1976
2.1. Nozione penalistica di raduno.....	1978
2.2. Nozione di pericolo e inclusione del nuovo reato di “raduni pericolosi” fra i delitti contro l’incolumità pubblica.....	1979
2.3. Il “rischio” di collisione con il diritto di riunione.....	1980
2.4. Riflessioni a margine di una “caduca” ipotesi criminosa.....	1982
3. Il “ <i>revirement</i> ” legislativo e la nuova versione del delitto di invasione di terreni o edifici per raduni pericolosi.....	1983
3.1. Le principali modifiche apportate dalla L. n. 199/2022.....	1985
3.2. Le ipotesi di responsabilità del promotore.....	1985
3.3. Il procedimento di constatazione (<i>alias</i> probatorio) della condizione di pericolo.....	1985
3.4. L’elemento psicologico ed il bilanciamento fra interessi/diritti affini.....	1986
3.5. Configurabilità del tentativo.....	1987
3.6. Concorso di reati.....	1988
3.7. L’applicabilità della confisca.....	1988
3.8. Spunti conclusivi in un’ottica di <i>de iure condendo</i>	1988
4. Profili processuali.....	1989
5. L’influenza dei profili sanzionatori sugli strumenti processuali penali e di controllo amministrativo.....	1990
6. La possibilità di disporre misure custodiali ed intercettazioni telefoniche.....	1992
7. Profili processuali dell’attuale 633- <i>bis</i> c.p.....	1995

L'estratto che stai consultando
fa parte del volume in vendita
su **ShopWKI**,
il negozio online di **Wolters Kluwer**

[Torna al libro](#)



CEDAM

IPSOA

UTET[®]
GIURIDICA

il fisco

 ALTALEX