

INDICE

pag.

Prefazione

XIII

I.

DIRITTO PENALE E INFORMATICA

1.1.	Informatica e diritto: punti di interazione	1
1.2.	L'Informatica giuridica	3
1.3.	Il Diritto dell'informatica	7
1.4.	L'ordinamento penale e l'informatica	10
1.5.	La normativa europea	14
1.6.	La legislazione italiana	19

II.

I REATI PREVISTI DALLE LEGGI N. 547/1993 E N. 48/2008

2.1.	Le norme penali riferite alla criminalità informatica	25
2.2.	La Legge 23 dicembre 1993, n. 547	27
2.3.	La Legge 18 marzo 2008, n. 48	29
2.4.	L'esercizio arbitrario delle proprie ragioni con violenza su un bene informatico	32
2.5.	Il danneggiamento ad impianti di pubblica utilità	34
2.6.	Il falso informatico	36
2.7.	Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri	38
2.8.	L'accesso abusivo ad un sistema informatico o telematico	40
2.9.	La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	44

2.10.	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	46
2.11.	La violazione della corrispondenza informatica	48
2.12.	I delitti di intercettazione informatica e telematica	50
2.13.	Il danneggiamento informatico	53
2.14.	La frode informatica	56

III.

LA TUTELA PENALE DEL DOMICILIO INFORMATICO

3.1.	L'accesso non autorizzato: la tutela prima della Legge 23 dicembre 1993, n. 547	65
3.2.	L'art. 4 della Legge n. 547/1993	67
3.3.	Valutazione dell'art. 4 nell'ottica dell'evoluzione del concetto di violazione domiciliare nell'ordinamento giuridico	68
3.4.	I concetti di «abitazione», «privata dimora» ed «appartenenze»	71
3.5.	I luoghi informatici	73
3.6.	Funzione strumentale della tutela giuridica del luogo informatico	75
3.7.	Il domicilio informatico	76
3.8.	L'acceso abusivo all'interno del sistema informatico o telematico protetto da misure di sicurezza	80
3.9.	La permanenza oltre i limiti consentiti, all'interno di un sistema protetto da misure di sicurezza	83
3.10.	Il sistema informatico e telematico	84
3.11.	Le misure di sicurezza	86
3.12.	Le aggravanti dell'art. 615-ter	89
3.13.	Il luogo del commesso reato ed il giudice competente in materia di accesso abusivo	91

IV.

I REATI INFORMATICI A SFONDO SESSUALE

4.1.	La rilevanza penale del sesso virtuale	95
------	--	----

	<i>pag.</i>
4.2. La pedofilia telematica	97
4.3. Le ragioni che spingono ad utilizzare la rete per fini “pedofili”	98
4.4. Tecnologie in rete e loro impiego per la distribuzione e cessione di materiale pedopornografico	99
4.5. Indirizzi sovranazionali e comunitari in materia di abuso e sfruttamento sessuale dei minori	100
4.6. La legislazione italiana riferita allo sfruttamento sessuale dei minori prima della Legge 3 agosto 1998, n. 269	102
4.7. La Legge 3 agosto 1998, n. 269 “Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù”	103
4.8. Le Leggi 38/2006 e 172/2012	104
4.9. La pornografia minorile	106
4.9.1. Il materiale pedopornografico	108
4.9.2. La pornografia virtuale	111
4.9.3. La distribuzione e cessione di materiale pedopornografico	112
4.9.4. L’eventuale responsabilità del <i>provider</i>	113
4.9.5. Le modifiche apportate dalla Legge n. 38/2006	117
4.10. La detenzione di materiale pedopornografico	117
4.11. L’attività di contrasto	123
4.12. Le iniziative turistiche nel <i>web</i> volte allo sfruttamento della prostituzione minorile	127
4.13. Istigazione a pratiche di pedofilia e di pedopornografia e adescamento dei minori	130
4.14. Sfruttamento e favoreggiamento della prostituzione <i>on line</i>	133
4.15. La violenza sessuale virtuale	136

V.

NUOVE FORME DI CRIMINALITÀ INFORMATICA

5.1. La criminalità informatica fenomeno proteiforme	139
5.2. Il <i>cyberstalking</i>	141
5.3. I reati informatici che esprimono odio	144

	<i>pag.</i>
5.4. La diffamazione on line	152
5.5. Il cyberbullismo	158
5.6. La diffusione illecita di immagini o video sessualmente espliciti (c.d. <i>revenge porn</i>)	163
5.7. Le nuove frontiere del Diritto penale dell'informatica: la responsabilità penale del <i>robot</i>	166

VI.

I REATI DI INTERNET

6.1. Rete e criminalità	169
6.2. Rete e norma penale	171
6.3. La rete come fonte di pericolo per i minori.	174
6.4. La rete come luogo privo di giurisdizione propria	177
6.5. La rete come strumento per garantirsi l'impunità	181
6.6. La rete sommersa	187
6.7. Il giudice penale nella rete	190
6.8. Sicurezza e libertà nella rete	195

VII.

IL REATO INFORMATICO IN AZIENDA

7.1. Il reato informatico come nuova minaccia per l'azienda	199
7.2. La criminalità informatica aziendale	201
7.3. L'impatto delle norme penali informatiche in ambito aziendale	203
7.4. La strategia aziendale per contrastare i reati informatici	205
7.5. Le valutazioni giuridiche in materia di sicurezza	206
7.5.1. La Legge 18 novembre 2019, n. 133	208
7.6. La polizza assicurativa quale rimedio per contenere il danno cagionato dal reato informatico	210
7.7. Valutazioni preliminari in ordine all'opportunità per l'azienda di denunciare il reato subito	211
7.8. La responsabilità dell'azienda per reati informatici commessi dai suoi vertici o dai suoi dipendenti a seguito dell'entrata in vigore del D.Lgs. n. 231/2001	213

	<i>pag.</i>
7.9. La Convenzione di Budapest e la Decisione Quadro 2005/222/GAI	216
7.10. Il reato informatico in azienda alla luce delle modifiche apportate dalla Legge 18 marzo 2008, n. 48	216
7.11. Come redigere la parte del modello riferita ai reati informatici	221

VIII.

CYBERTERRORISMO, *CYBERWAR*, MAFIA DIGITALE

8.1. Terrorismo e informatica	225
8.2. Il cyberterrorismo	227
8.3. I cyberterroristi	228
8.4. L'uso delle reti per finalità terroristiche	230
8.5. Le norme antiterrorismo	232
8.6. Le principali questioni di diritto processuale poste dalla cybercriminalità	235
8.7. <i>Cyberwar</i>	239
8.8. Le maggiori questioni giuridiche poste dalla <i>cyberwar</i>	243
8.9. Mafia digitale	245

IX.

IL REATO INFORMATICO NEL PROCESSO PENALE

9.1. L'interpretazione del delitto informatico	249
9.2. Il delitto informatico nelle indagini preliminari	251
9.3. <i>La Digital Forensics</i>	253
9.4. I mezzi di ricerca della prova	255
9.5. Le misure cautelari reali in materia informatica	260
9.6. Il reato informatico nel giudizio penale	265
9.7. Il giudice ed i condizionamenti di carattere tecnico.	266
9.8. Il giudice ed i condizionamenti che derivano dal modo di interpretare le tecnologie	270
9.9. Il giudice ed i condizionamenti di carattere "politico"	276

X.

NUOVE PSICOPATOLOGIE E RIPERCUSSIONI
SULL'ACCERTAMENTO DELLA COLPEVOLEZZA
INFORMATICA

10.1. Le tecnologie dell'informazione e la percezione della vittima	281
10.2. Le tecnologie dell'informazione e la percezione del reato	283
10.3. Tecnologie dell'informazione e movente "politico"	285
10.4. L'imputabilità del delinquente informatico	286
10.5. I motivi a delinquere del cybercriminale	289
Postfazione di Eugenio Albamonte	293