

# INDICE

	<i>pag.</i>
<i>Introduzione</i>	XI
 CAPITOLO 1 REATI INFORMATICI  	
1.1. I reati “necessariamente informatici” previsti dall’ordinamento giuridico italiano	1
1.2. La violazione del “domicilio informatico”	4
1.2.1. L’accesso abusivo a sistema informatico o telematico (art. 615-ter c.p.)	4
1.2.2. Detenzione e uso di mezzi idonei all’accesso abusivo (art. 615-quater c.p.)	6
1.3. L’alterazione delle comunicazioni telematiche e informatiche	8
1.3.1. Intercettazione, impedimento o interruzione illecita di comunicazioni e uso dei relativi mezzi (artt. 617-quater e 617-quinquies c.p.)	8
1.3.2. Falsificazione, alterazione o soppressione di comunicazioni informatiche (art. 617-sexies c.p.)	10
1.4. Il danneggiamento di dati e sistemi informatici	11
1.4.1. Il danneggiamento di informazioni, dati e programmi informatici (artt. 635-bis e 635-ter c.p.)	11
1.4.2. Il danneggiamento di sistemi informatici o telematici (artt. 635-quater, 635-quater.1, 635-quinquies e c.p.)	13
1.5. La frode informatica	16
1.5.1. La frode informatica (640-ter c.p.) e la truffa online (640 c. 2-ter)	16
1.5.2. Il <i>phishing</i>	19
1.5.3. Il <i>pharming</i>	23
<i>Riferimenti bibliografici</i>	24

## CAPITOLO 2 CYBERCRIMES

2.1.	Al di là dei reati necessariamente informatici	27
2.2.	Il <i>cyberstalking</i>	28
2.3.	La pornografia digitale	30
2.3.1.	<i>Sexting</i> e <i>sextortion</i>	30
2.3.2.	Pedopornografia, adescamento di minori e pornografia virtuale	32
2.3.3.	Pornografia non consensuale ( <i>revengeporn</i> )	34
2.4.	Il cyberbullismo	36
2.5.	I discorsi d'odio online ( <i>hate speech</i> )	38
2.6.	Le <i>fake news</i>	40
2.7.	Gli illeciti contro la <i>privacy</i>	42
2.8.	<i>Malware-as-a-Service</i> e DDoS	43
2.9.	I <i>ransomware</i>	46
2.10.	Il <i>cyberlaundering</i>	48
	<i>Riferimenti bibliografici</i>	51

## CAPITOLO 3 GUERRA CIBERNETICA

3.1.	Le trasformazioni della guerra e la <i>cyberwar</i>	53
3.2.	Il problema della qualificazione giuridica della <i>cyberwar</i> : i Manuali di Tallinn	55
3.2.1.	La <i>Web War One</i>	55
3.2.2.	Il Manuale di Tallinn	57
3.2.3.	Il Manuale di Tallinn 2.0	61
3.3.	Le <i>cyberweapons</i>	62
3.4.	I <i>cyberwarriors</i>	65
3.4.1.	Combattenti cibernetici statali	66
3.4.2.	Combattenti cibernetici parastatali	67
3.4.3.	Combattenti cibernetici transnazionali	68
	<i>Riferimenti bibliografici</i>	70

## CAPITOLO 4 PIRATI E TERRORISTI NELL'ERA DIGITALE

4.1.	Pirati e terroristi. Due figure dell'inimicizia assoluta	73
4.2.	La pirateria informatica	75

	<i>pag.</i>
4.2.1. Il mare di silicio	75
4.2.2. Il nemico del <i>copyright</i>	76
4.2.3. Chi ha paura del pirata informatico?	77
4.3. Cyberterrorismo e terrorismo convenzionale	80
4.4. Terrorismo e tecnologie informatiche	82
4.4.1. Terrorismo per il web. Propaganda, reclutamento, addestramento	82
4.4.2. Web per il terrorismo. Pianificazione e <i>dark markets</i>	85
<i>Riferimenti bibliografici</i>	86

## CAPITOLO 5 INFORMATICA FORENSE

5.1. Informatica forense e <i>digital evidence</i>	89
5.1.1. Definizioni	89
5.1.2. Acquisizione dei dati per l'analisi forense	91
5.2. Convenzione di Budapest e legge 48/2008: i mezzi di ricerca della prova digitale	93
5.2.1. Ispezione	94
5.2.2. Perquisizione	95
5.2.3. Sequestro e intercettazioni	96
5.3. Un caso esemplare. Il delitto di Garlasco	98
<i>Riferimenti bibliografici</i>	101

## CAPITOLO 6 CYBERSECURITY

6.1. La sicurezza cibernetica come problema globale	103
6.2. <i>Cybersecurity</i> e Unione Europea	104
6.2.1. Direttiva ECI e infrastrutture critiche europee	104
6.2.2. La strategia dell'Unione Europea per la sicurezza cibernetica: direttiva NIS e regolamento 2019/881 ( <i>Cybersecurity Act</i> )	106
6.2.3. Una nuova strategia: verso la direttiva NIS2	108
6.3. L'approccio italiano alla <i>cybersecurity</i>	112
6.3.1. La "legge perimetro"	112
6.3.2. La difesa dello spazio cibernetico italiano	114
6.3.3. Agenzia per la cybersicurezza nazionale (ACN)	115
6.3.4. NIS2: una sfida per il Paese	118
<i>Riferimenti bibliografici</i>	120

