

Indice

Prefazione	XI
Capitolo I. <i>Cybersecurity</i>: contesto normativo di riferimento a livello nazionale ed europeo.	1
<i>Giuseppe Cassano - Michele Iaselli</i>	
1. La sicurezza informatica	1
2. La convenzione di Budapest	4
3. Sicurezza informatica e <i>privacy</i> : un connubio necessario	6
4. I primi provvedimenti in materia di <i>cybersecurity</i> nella PA e la Direttiva NIS	9
5. Il perimetro di sicurezza nazionale cibernetica.	13
6. La nascita dell’ <i>Agenzia per la cybersicurezza</i> nazionale e la strategia nazionale di <i>cybersicurezza</i>	15
7. Il Regolamento sulla <i>cybersicurezza</i> 2019/881/UE	23
Capitolo II. <i>Cybersecurity</i>, protezione dei dati personali, diritto penale	27
<i>Andrea Mattarella</i>	
1. La rivoluzione informatica e i nuovi scenari criminali	27
2. Il Regolamento 2016/679/UE e la tutela penale della <i>privacy</i>	32
3. Il rischio di <i>bis in idem</i> tra reato e illecito amministrativo	39
4. La responsabilità da reato “informatico” degli enti e la <i>privacy</i>	42
5. I modelli organizzativi e le misure di contenimento del rischio di violazione di dati personali: il necessario confronto tra il D.Lgs. 8 giugno 2001, n. 231 e il Regolamento 2016/679/UE.	46
6. DPO e ODV. Interferenze e profili differenziali	50
Capitolo III. <i>Cyberspazio</i> e <i>onlife</i>: dalle origini della Costituzione alla società digitale.	55
<i>Rosa Tarricone</i>	
1. <i>Cyberspazio</i> e <i>onlife</i> : <i>ubi societas technologica, ibi ius</i>	55
2. L’impatto della digitalizzazione sul principio di separazione dei poteri dello Stato »	58
3. I diritti costituzionali nell’era digitale: una Costituzione per <i>Internet</i> ?	63
3.1. Il diritto di accesso ed il fenomeno del c.d. <i>digital divide</i>	66
3.2. (<i>Segue</i>) Il diritto alla libertà di manifestazione del pensiero	72

3.3. (<i>Segue</i>) Il diritto alla <i>privacy</i> e la protezione dei dati personali e sensibili	76
3.4. (<i>Segue</i>) Il diritto all'oblio.	80
4. Alcune riflessioni sul processo (ancora incompiuto) di digitalizzazione	85
Capitolo IV. Scenari: <i>cybercrime</i>, mafie, riciclaggio	89
<i>Ranieri Razzante</i>	
1. I modelli della criminalità informatica organizzata	89
2. <i>Cyber Organised Crime</i> : la complessità delle attività criminali nel <i>cyberspace</i>	90
3. La criminalità organizzata italiana all'estero e le relazioni internazionali	94
4. Le valute virtuali: criticità e rischi di riciclaggio di denaro	98
5. L'utilizzo criminale delle piattaforme di pagamento	101
Capitolo V. Strumenti di contrasto alla criminalità informatica a livello nazionale ed europeo	111
<i>Filippo Bosi</i>	
1. Una ricognizione della normativa di riferimento. <i>Brevi cenni</i>	111
2. La Legge 15 febbraio 2012, n. 12: criminalità informatica e confisca	115
3. Il coordinamento investigativo internazionale: Europol, Interpol.	117
4. Strategie intra e intergovernative di <i>cyberterrorism</i>	121
5. La cooperazione multilaterale di polizia – progetto ICAN.	124
6. La Rete Europea Antimafia <i>Operational Network@ON</i> – progetto ONNET.	125
7. Possibili strategie di intervento in tema di diritto penale nell'ambito dell'Unione europea e dell'Italia.	127
Capitolo VI. La Convenzione delle Nazioni Unite contro il <i>cybercrime</i>: l'ultima frontiera del contrasto alle nuove forme di criminalità transnazionale	131
<i>Andrea Mattarella</i>	
1. L'ineffettività della Convenzione di Budapest e il ruolo " <i>suppletivo</i> " della Convenzione di Palermo	131
2. L'importanza di una Convenzione Onu in materia di <i>cybercrime</i> e il lungo percorso dei lavori	137
3. Le relazioni presentate dagli Stati	140
Capitolo VII. La <i>blockchain</i>	151
<i>Maria Bruccoleri</i>	
1. <i>Web Revolution</i>	151
2. Come funziona la <i>blockchain</i> : elementi e caratteristiche	152

3. I vantaggi della tecnologia <i>blockchain</i> »	154
4. Le applicazioni della <i>blockchain</i> : il successo nel suo utilizzo »	155
5. Le tipologie di reti <i>blockchain</i> »	158
Capitolo VIII. Gli <i>smart contract</i> »	161
<i>Maria Bruccoleri</i>	
1. Concetto di <i>smart contract</i> : cosa sono e come funzionano »	161
2. <i>Smart contract</i> : una nuova opzione nella legge dei contratti »	163
3. <i>Blockchain</i> e <i>smart contract</i> »	164
4. Modelli di consenso decentralizzato e di informazione distribuita. »	165
5. <i>Smart contract application</i> »	169
6. Potenziale e opportunità di applicazione: cittadini, governi e imprese. »	172
Capitolo IX. L'attribuzione degli attacchi informatici e il <i>cyberterrorismo</i> »	177
<i>Ranieri Razzante</i>	
1. Il Metaverso: un <i>locus commissi delicti</i> atipico »	177
2. Gli attacchi informatici: le minacce del nuovo millennio. »	179
3. Le tre fasi dell'attribuzione. La fase tecnica. »	179
4. (<i>Segue</i>) La fase politica. »	180
5. (<i>Segue</i>) La fase giuridica. »	180
6. La normativa europea: il Regolamento 2019/796/UE »	182
7. Il fenomeno del <i>cyberterrorismo</i> »	183
8. (<i>Segue</i>) La <i>cybersicurezza</i> in Italia. »	190
9. Direttiva NIS (<i>Network and Information Security</i>). »	192
10. Direttiva NIS 2: i cambiamenti »	193
11. Attacchi informatici ed attuale panorama sanzionatorio italiano: prospettive <i>de iure condendo</i> »	195
12. Impiego dell'intelligenza artificiale per gli attacchi informatici. Un'attribuzione sempre più ardua. »	197
Capitolo X. Il ruolo della criminologia nella <i>cybersecurity</i> »	201
<i>Fabio Giannini</i>	
1. Conoscere e comprendere la <i>cybersecurity</i> »	201
2. <i>Cybercrime</i> : metodologie criminali approcciate alla criminologia. »	202
3. Evoluzione e devianza delle tecniche di <i>hacking</i> »	204

Capitolo XI. Profili legali e <i>best practice</i> della cybersecurity in ambito assicurativo	209
<i>Chiara D’Antò - Alessandro Romagnolo</i>	
1. Ricognizione della disciplina	209
2. Il <i>cyber risk assessment</i>	210
3. Il coordinamento con la normativa <i>privacy</i>	213
4. L’assicurazione contro gli attacchi <i>cyber</i>	214
5. Il caso Acer: attacco <i>ransomware</i> per vulnerabilità di <i>Exchange</i>	216
6. Le <i>best practices</i> nel mondo <i>cyber</i>	217
7. I (buoni) propositi del Legislatore	220
Capitolo XII. Intelligenza artificiale e diritto: algoritmi, giustizia predittiva e giudici robot	223
<i>Rosa Tarricone</i>	
1. La storia dell’intelligenza artificiale: cos’è e come funziona	223
2. <i>Machine Learning</i> e <i>Deep Learning</i> : tra intelligenza artificiale debole e forte	227
3. Le basi dell’AI: la definizione di algoritmo	233
3.1. I principi del processo decisionale automatizzato: tra equità e discriminazione.	242
4. La <i>Governance</i> dell’AI, uno sguardo al futuro	247
5. Nuove tecnologie ed etica: l’apporto umano è ancora necessario?	252
6. La predittività delle decisioni: l’acceso dibattito circa l’ammissibilità dell’algoritmo giudicante	256
7. L’AI come strumento di risoluzione delle controversie giudiziarie: limiti all’applicazione della giustizia predittiva	261
8. Interpretazione della legge con modelli matematici	265
9. Il primo magistrato-robot in Estonia e in Cina	271
10. Il sistema giudiziario italiano nelle mani dell’AI: uno scenario possibile?	275
Capitolo XIII. <i>Security awareness</i>	285
<i>Adriano Proscia</i>	
1. Cosa è la <i>security awarness</i>	285
2. Paradigmi di comunicazioni in rete	290
2.1. (<i>Segue</i>) Il paradigma <i>client – server</i>	291
2.2. (<i>Segue</i>) Il paradigma <i>peer-to-peer: Distributed Ledger Technology e Blockchain</i>	292
2.3 (<i>Segue</i>) Il paradigma <i>cloud computing</i>	299
3. Comprendere le minacce informatiche	303

3.1. (Segue) <i>Ransomware</i> »	304
3.2. (Segue) <i>Privilege Escalation</i> »	306
3.3. (Segue) <i>Distributed Denial of Service</i> »	307
3.4. (Segue) <i>Attacchi social media</i> »	310
3.5. (Segue) <i>Man in the Middle</i> »	311
3.6. (Segue) <i>Phishing</i> »	312
4. <i>Le best practices</i> che possono preservarci »	314
5. Strategie e piani per gestire eventi inaspettati. »	317
Capitolo XIV. Tutelare i minori nell'era digitale »	323
<i>Francesca Del Gaudio</i>	
1. I minori, soggetti (anche) tecnologicamente vulnerabili »	323
2. Il fenomeno del <i>cyberbullismo</i> »	325
3. Relazione tra minori e diritto alla <i>privacy</i> »	330
4. Cenni di diritto penale: l'adescamento di minori... attraverso la rete »	335
Capitolo XV. Appendice normativa. Le Linee Guida per la Cybersicurezza »	341
<i>Giorgia Azzellini - Ines Castellet y Ballarà</i>	
1. Riferimenti nazionali »	341
2. Riferimenti sovranazionali »	349
3. Fonti internazionali »	357
4. Cenni di comparazione »	359
Autori »	361