

Indice

Premessa XIII

UNITÀ 1 IL CONTROLLO E LA SORVEGLIANZA NELLA SOCIETÀ DIGITALE

Capitolo I

Controllo, sorveglianza e segreto: una prospettiva informatico-giuridica

di *Giovanni Ziccardi*

1. Premesse	3
2. La società sorvegliata	4
3. Il ruolo dell'interprete	6
4. I possibili rimedi	8
5. Alcune conclusioni	9

Capitolo II

Sorveglianza di massa e tutela dei diritti fondamentali

di *Pierluigi Perri*

1. Il difficile bilanciamento tra il diritto al rispetto della vita privata e familiare e la sorveglianza di massa	11
2. L'articolo 8 della CEDU nella giurisprudenza della Corte Europea dei Diritti dell'Uomo	13
3. Le eccezioni previste dal comma 2 dell'articolo 8 CEDU e il bilanciamento tra tutela della vita privata e sicurezza nazionale	15
4. L'inquadramento della sorveglianza di massa nella sentenza della Corte di Giustizia Europea sul caso Schrems	19
5. Conclusioni	20

Capitolo III

La "società liquida" e il caso Snowden

di *Gabriele Suffia*

1. Dal mondo analogico alla società liquida: la sorveglianza e il controllo come fondamento del sistema	23
2. Le basi giuridiche del controllo dei dati: le due vie	25
3. Accordo tra Stati e il paradigma Echelon	27
4. Accordo tra Stati e privati: il caso Snowden	32

5. Conseguenze del caso Snowden e l'affermazione di un nuovo tipo di "trasparenza" 36

Capitolo IV

Leaking, whistleblowing e il caso WikiLeaks

di *Kateryna Fedorova*

1. Leaking e whistleblowing 41
2. La disciplina del whistleblowing in Italia 42
3. WikiLeaks e le rivelazioni più significative 45
4. WikiLeaks e le sue attività. 50

Capitolo V

Videosorveglianza e controllo dei dati del cittadino e del lavoratore

di *Mirko Pizzocri*

1. Il controllo dei lavoratori, l'articolo 4 e l'impianto normativo precedente all'entrata in vigore del Jobs Act 53
2. Il rinnovato articolo 4 tra modifiche lessicali, strumentali e sanzionatorie. 57
3. L'evoluzione normativa della videosorveglianza del cittadino (dalla sua genesi sino al GDPR) 61

Capitolo VI

La profilazione, Cambridge Analytica e il micro-targeting

di *Simone Bonavita*

1. La profilazione 65
2. Cambridge Analitica 72
3. Il micro-targeting 74

UNITÀ 2

I CRIMINI INFORMATICI, GLI ILLECITI CON L'USO DELLA RETE E L'ODIO INTERPERSONALE

Capitolo VII

I reati informatici

di *Pierluigi Perri*

1. La difficile regolamentazione dei reati informatici 79
2. La Convenzione di Budapest sulla criminalità informatica e la legge n. 48/2008 84
3. L'accesso abusivo ad un sistema informatico o telematico 88

Capitolo VIII

Gli aspetti informatico-giuridici del cyberstalking

di *Marcello Bergonzi Perrone*

1. Definizioni e inquadramento normativo 97
2. Analisi della fattispecie. 99
3. L'aggravante di cyberstalking prevista dal secondo comma dell'art. 612-*bis* c.p. 101
4. Le caratteristiche peculiari del cyberstalking 105

Capitolo IX

Il cyberbullismo tra diritto e nuove tecnologie

di *Samanta Stanco*

1. Introduzione. 109
2. Le origini del fenomeno 110
3. Le condotte tipiche. 113
4. Il quadro normativo in Italia 117
5. Una comparazione tra bullismo e cyberbullismo 121

Capitolo X

Il contrasto al cyberbullismo tra cultura e percorsi formativi

di *Giovanni Ziccardi*

1. Alcune premesse 123
2. Il profilo degli aggressori e delle vittime online. 125
3. I cambiamenti portati dalle relazioni digitali 127
4. Una proposta di percorso formativo per il contrasto al cyberbullismo 131
5. Alcune conclusioni 136

Capitolo XI

L'adescamento di minorenni e il grooming

di *Athena Skoufas*

1. L'adescamento di minorenni: la Convenzione di Lanzarote e l'art. 609-*undecies*. 139
2. Le fasi del *grooming* online 143
3. Il profilo dell'adescatore 146
4. Il profilo della vittima 148

Capitolo XII

Le espressioni d'odio online

di *Giovanni Ziccardi*

1. Alcune considerazioni introduttive 153

2.	Il delicato rapporto tra odio, web e piattaforme online	154
3.	L'odio politico è facilitato dalla rete stessa?.	157
4.	Le caratteristiche originali dell'odio politico online	160
4.1.	La capacità amplificatrice e diffusiva dell'odio politico	161
4.2.	La persistenza delle informazioni nell'ambiente digitale.	162
4.3.	Lo schermo quale scudo dietro il quale parlare (e proteggersi) . .	163
4.4.	L'anonimato come (percepita) protezione.	163
4.5.	Odio più creativo e facilitato grazie alle tecnologie	163
4.6.	Odio post-moderno aggregato e connesso.	164
4.7.	La rete quale nuovo teatro per le azioni d'odio	165
5.	La rete quale strumento di contrasto all'odio online.	165
6.	L'odio come valuta e come mercato	169
7.	La capacità di autodifesa degli utenti e della rete	170
8.	L'intervento dello Stato e il ruolo dei provider.	171
9.	Conclusioni: il delicato rapporto tra controllo dell'odio e diritti di libertà.	174

Capitolo XIII

La diffamazione online e il furto di identità

di *Andrea Scirpa*

1.	La diffamazione online.	179
2.	Il furto d'identità	186

Capitolo XIV

Il negazionismo in Internet, nel deep web e sui social network: evoluzione e strumenti di contrasto

di *Giovanni Ziccardi*

1.	L'articolato rapporto tra negazionismo e reti telematiche	193
2.	Negazionismo, social network e nuovi media	194
3.	Il negazionismo dalle prime BBS al deep web	197
4.	Amplificazione, diffusione, reti sociali, persistenza, scelta della giurisdizione.	198
5.	Conclusioni: la controparola, il diritto e la tecnologia quali possibili strumenti di contrasto al negazionismo in rete?	200

UNITÀ 3

LA CYBERSECURITY, LA GUERRA DELL'INFORMAZIONE E IL CYBERTERRORISMO

Capitolo XV

La cybersecurity nel quadro tecnologico (e politico) attuale

di *Giovanni Ziccardi*

1.	Un pericoloso intreccio tra politica e cybersecurity e l'emergere degli APT.	207
----	--	-----

2. La nuova cybersecurity e le minacce più comuni.	209
--	-----

Capitolo XVI

La protezione dalle frodi, dal phishing e dalle estorsioni online

di *Antonio Sagliocca*

1. Introduzione.	211
2. Il <i>social engineering</i>	213
3. Le tipologie di frodi più comuni	214
4. La protezione dalle truffe online	216
5. Il <i>phishing</i> , lo <i>spear phishing</i> e il <i>whaling</i>	219
6. La protezione della posta elettronica.	221
7. Le estorsioni online.	223
8. La difesa dalle estorsioni online.	224

Capitolo XVII

La protezione dal malware

di *Paolo Dal Checco*

1. Introduzione.	225
2. Terminologia e tipi di minacce	226
3. Strumenti per la protezione	228
4. Consigli comportamentali e precauzioni d'uso	231
5. Strumenti e consigli per il recupero delle funzionalità e dei dati.	233

Capitolo XVIII

Il deep web e il dark web

di *Yvette I. Agostini*

1. Introduzione.	237
2. Il web di superficie (<i>surface web</i>) e il deep web	237
3. TOR, I2P, Freenet e le dark net	238
4. Le precauzioni da adottare nell'accesso al dark web e i suoi utilizzi.	240
5. Alcune conclusioni	243

Capitolo XIX

La direttiva NIS, la security per l'Industria 4.0 e la transizione al digitale

di *Giuseppe Giorgio Pacelli*

1. Il valore dell'informazione.	245
2. Transizione al digitale: digitalizzazione o trasformazione	246
3. Data leadership	247
4. Dalla Direttiva UE 2016/1148 al d.lgs 65/2018: sicurezza delle reti e dei sistemi informatici	251
5. Human risk management	254

Capitolo XX

L'uso di policy ai fini di sicurezza informatica

di *Giovanni Ziccardi*

1. L'importanza di un set d'istruzioni nel "sistema" GDPR 257
2. Un esempio di istruzioni sull'uso degli strumenti informatici e le misure adeguate di sicurezza. 258
3. Un esempio di istruzioni sulla gestione interna ed esterna di possibili data breach 263
4. Un esempio di istruzioni miranti alla protezione dagli attacchi di phishing. 266
5. Alcune considerazioni conclusive. 269

Capitolo XXI

Gli scenari attuali della guerra dell'informazione

di *Stefano Mele*

1. Il ruolo del ciberspazio nello scenario attuale della guerra dell'informazione 271
2. Il livello di minaccia e gli obiettivi delle *Cyberspace Operations* 273
3. Le *Cyberspace Operations* nel contesto internazionale 278
4. *Cyberspace Operations* e governo italiano 285

Capitolo XXII

Fake news e disinformazione

di *Gabriele Suffia*

1. La "fake news" nel quadro dell'informazione oggi. 293
2. Esempi di disinformazione e casi studio. 296
3. Disinformazione e social network. 298
4. Disinformazione e diritto 299

Capitolo XXIII

Guerra dell'informazione e politica

di *Giovanni Ziccardi*

1. Premesse. 303
2. La politica sui social network. 304
3. I lati oscuri 307
4. Una nuova attenzione all'etica? 309

Capitolo XXIV

Cyberterrorismo e radicalizzazione online

di *Stefano Mele*

1. Il ruolo di Internet e delle tecnologie nelle attività terroristiche 313
2. L'al-Qaida di bin Laden e Internet. 315

3. L'ISIS di al-Baghdadi e Internet 317
4. La risposta italiana al terrorismo cibernetico 321

UNITÀ 4

LE INVESTIGAZIONI NELL'ERA DIGITALE

Capitolo XXV

Gli aspetti informatico-giuridici delle investigazioni digitali

di *Giovanni Ziccardi*

1. Il quadro attuale 329
2. La Convenzione di Budapest e le prime regole pratiche. 331
3. Le linee di ricerca 333

Capitolo XXVI

Le basi della digital forensics

di *Ferdinando Ditaranto*

1. Le scienze forensi e la nascita della digital forensics 337
2. Le peculiarità della digital evidence 340
3. La digital forensics e il ruolo dell'informatico forense. 346

Capitolo XXVII

Il captatore informatico: alcune riflessioni informatico-giuridiche

di *Giovanni Ziccardi*

1. Il captatore al centro del dibattito politico e legislativo attuale: alcune premesse necessarie. 355
2. Il quadro precedente alla "Riforma Orlando" 359
3. La nuova disciplina del captatore nella "Riforma Orlando" 360
4. Gli aspetti informatico-giuridici più dibattuti. 363
5. Alcune riflessioni conclusive. 368

Capitolo XXVIII

Un'introduzione alla Social Network Analysis

di *Alessandro Massaro*

1. Introduzione. 371
2. Le basi della *social network analysis* 372
3. La *social network analysis* applicata alle reti criminali 376

Gli Autori di questo Volume. 383