

Indice

Introduzione	11
<i>Parte prima. DIRITTO E TRASFORMAZIONE DIGITALE</i>	21
I. Società tecnologica, sensori e diritto	23
1. La società dei sensori	23
2. I metadati	27
3. La data retention	29
4. La profilazione	31
5. L'Internet delle cose	33
6. Gli assistenti digitali	35
7. La fiction	37
II. Controllo tecnologico e sorveglianza liquida	41
1. Controllo e sorveglianza nell'era tecnologica	41
2. La protezione dei dati	44
3. L'uomo di vetro	46
4. I controlli a distanza	48
5. L'11 settembre	49
6. I social network	50
7. Lo smartphone, gli algoritmi e i colossi di Internet	50
8. Il Datagate	51
9. L'Internet delle cose, la domotica, i big data e i sensori	52
10. Cambridge Analytica e il machine learning	53
11. L'era della pandemia e l'avvento dell'intelligenza artificiale	55
12. Controllo orwelliano e controllo kafkiano	55
13. Shoshana Zuboff e il capitalismo della sorveglianza	58
III. Il giurista e la scienza dei dati	63
1. Il dato	63
2. I big data e il loro ecosistema	65
3. L'automazione dei trattamenti	68
IV. La mercificazione delle informazioni	73
1. Paranoici <i>vs</i> esibizionisti	73
2. Il mercato dei dati personali	79
3. L'esposizione del lato più intimo	81
4. Il neoliberismo digitale	84

Indice

V.	Il diritto della rete	89
	1. Il pensiero di Stefano Rodotà	89
	2. Una Dichiarazione europea su diritti e principi digitali e una <i>Internet Bill of Rights</i>	94
	<i>Parte seconda. I DIRITTI DELL'INFORMATICA</i>	103
VI.	La violazione dei diritti	105
	1. Il necessario intervento del legislatore	105
	2. La regolamentazione della profilazione segreta	106
	3. La violazione dei diritti	108
	4. La tecnologia per resistere	110
	5. Il mutamento dei comportamenti	111
	6. La protezione dei dati altrui	113
	7. I tempi attuali	114
VII.	La regolamentazione giuridica dell'informatica	119
	1. La disciplina giuridica delle nuove tecnologie	119
	2. Il copyright, il diritto d'autore e i prodotti digitali	120
	3. I principi della "Direttiva copyright"	124
	4. La protezione dei dati	125
	5. La cybersecurity e la protezione delle infrastrutture critiche con la NIS2	126
	6. Il commercio elettronico	126
	7. I crimini informatici, il terrorismo e i contenuti d'odio	128
	8. I minori tra bullismo, adescamento e pedopornografia	129
	9. L'idea di una pubblica amministrazione digitale	130
	10. L'intelligenza artificiale e la sua regolamentazione	132
	11. La resilienza del settore finanziario e il regolamento DORA	134
VIII.	Unione europea, società digitale e diritto	137
	1. La politica dell'Unione europea per il digitale	137
	2. L'intelligenza artificiale etica o "all'europea"	137
	3. La strategia europea in materia di dati	139
	4. La politica industriale, il green tech e la nuova agricoltura	139
	5. La normativa sui mercati digitali	140
	6. La normativa sui servizi digitali	141
	7. La cybersecurity	142
	8. Le auto senza conducente, le strade intelligenti e la mobilità nel futuro	144
	9. Gli open data, i linked open data e la "liberazione" dei dati pubblici	146
IX.	I dati, l'intelligence e il law enforcement	149
	1. Edward Snowden e il Datagate	149
	2. Il ruolo dei contractor privati	150
	3. Cyberintelligence, cybersecurity e cloud	151
	4. La diffusione dei segreti	152

X.	Le minacce	157
	1. Strani acquisti notturni	157
	2. Gli attacchi informatici	158
	3. Il phishing	161
	4. La conoscenza	161
	5. L'analisi del testo	162
	6. I messaggi mirati	164
	7. Le credenziali	164
	8. I dati bancari	165
	9. I link e gli allegati	166
	10. L'utilità dell'antivirus	166
	11. Il superamento del senso di vergogna	167
	12. Kevin Mitnick e la <i>human security</i>	167
	<i>Parte terza. IL GIURISTA DEL FUTURO</i>	173
XI.	L'informatica giuridica	175
	1. L'importanza dell'informatica giuridica	175
	2. Enrico Pattaro e la scuola bolognese	176
	3. Mario Jori e l'informatica giuridica all'Università di Milano	178
	4. I diritti delle nuove tecnologie	182
	5. L'esperienza didattica	183
	6. Un approccio corretto alla materia	185
	7. Il futuro dell'informatica giuridica in otto aree di ricerca milanesi	189
	8. L'importanza – e il pregio – dell'interdisciplinarietà	194
	9. Dall'informatica giuridica al legal tech	194
XII.	Il legal tech e il legal design	197
	1. Il legal tech	197
	2. Un volano per le professioni del futuro	199
	3. Il legal design	200
XIII.	Il giurista-programmatore	205
	1. I corsi di <i>coding for lawyers</i>	205
	2. Perché studiare la programmazione a Giurisprudenza	206
XIV.	La cybersecurity	209
	1. Le competenze in cybersecurity	209
	2. L'autenticazione e le password	211
	3. La sicurezza della postazione di lavoro	213
	4. L'importanza dei comportamenti	216
	5. La protezione del cloud	216
	6. Il <i>cybersecurity lawyer</i> e la sua formazione	217
XV.	Il Data Protection Officer	219
	1. La figura del Data Protection Officer (DPO) e le norme di riferimento	219

	2. La formazione del DPO	223
	3. Il ruolo del DPO nella gestione dei data breach	224
XVI.	La regolamentazione europea dell'intelligenza artificiale	231
	1. Il presente dell'intelligenza artificiale	231
	2. Il regolamento	231
	3. Il rispetto dei diritti fondamentali	233
	4. L'ambito di applicazione	234
	5. Le pratiche vietate	235
	6. I sistemi ad alto rischio	236
	7. Gli obblighi di trasparenza	237
XVII.	L'Open Source Intelligence (OSINT), il deep web e le botnet	239
	1. L'uso di tecniche di OSINT	239
	2. Deep web e dark web	241
	3. Le botnet	241
XVIII.	Segreto e riservatezza	243
	1. Ottenere segreto e riservatezza	243
	2. Tor e la navigazione anonima	244
	3. La posta elettronica e il cloud cifrati	248
	4. L'uso di una Virtual Private Network (VPN)	249
	5. Le funzioni di Tails	250
	6. Il whistleblowing e SecureDrop	251
	7. La cifratura, l'anonimizzazione e il wiping dei dati	253
XIX.	La persistenza, la rimozione, la falsità e l'immortalità dei dati	257
	1. Il problema della persistenza dei contenuti online e il diritto all'oblio	257
	2. La cancellazione dei dati	261
	3. Le linee guida su Google Spain	262
	4. I criteri per domandare la deindicizzazione	263
	5. L'eredità digitale	267
	6. Il deep fake	268
XX.	La presenza sui social media	273
	1. Nuovi mezzi di comunicazione e professione legale	273
	2. Una <i>social media ethics</i> per gli avvocati	278
	3. Le dodici regole dell'American Bar Association	282
	4. Un'ipotesi di <i>social media policy</i> per lo studio legale	283
	5. Comportarsi bene in rete: la netiquette di Giancarlo Livraghi	284
	6. Gli avvocati e l'intelligenza artificiale generativa	286
XXI.	I minori digitali e il family tech	289
	1. I minori, la vita in famiglia e il family tech	289
	2. Le sfide pericolose e il sexting	290

	<i>Indice</i>
3. Cyberbullismo, cyberstalking e revenge porn	293
4. Le fake news e gli adolescenti	302
5. La tutela dei dati dei minori nel GDPR e la loro profilazione	304
6. Le regole di difesa e un futuro connotato dall'intelligenza artificiale	309
XXII. La <i>computer ethics</i>	313
1. Il ritorno della <i>computer ethics</i>	313
2. Il codice della Association for Computing Machinery (ACM)	317
3. Una visione moderna dell'etica informatica	317
4. Il problema specifico dei contenuti d'odio online	320
XXIII. La criminalità tecnologica	323
1. I crimini informatici	323
2. Il Chaos Computer Club e la scena hacker tedesca	326
3. La natura degli attacchi	329
4. Il panorama attuale	332
5. United States <i>vs</i> Aaron Swartz	333
6. Alcune riflessioni sul futuro (e sull'intelligenza artificiale)	338
Conclusioni	341
Bibliografia	343
Indice analitico	353