

# INDICE

INTRODUZIONE	»	3
CAPITOLO 1		
I PRINCIPI COSTITUZIONALI E SOVRANAZIONALI DELLA RISERVATEZZA E DELLA SICUREZZA DEI DATI PERSONALI	»	5
1. La sicurezza come diritto di libertà e il ruolo della privacy nel prossimo futuro	»	5
2. Brevi cenni storici: la storia del diritto alla riservatezza	»	8
CAPITOLO 2		
LA SICUREZZA E LA PRIVACY	»	15
1. La riservatezza della persona e riservatezza dei dati sono anche concetti di sicurezza	»	15
2. Il concetto di dato personale	»	22
3. Il dato giudiziario	»	33
4. Il concetto di trattamento dei dati personali	»	35
CAPITOLO 3		
IL REGOLAMENTO GENERALE (UE) PER LA PROTEZIONE DEI DATI PERSONALI DEL 2016, N. 679	»	37
1. Il nuovo regolamento Europeo sul trattamento dei dati (GDPR) e il Codice per la protezione dei dati personali: appunti	»	38
1.1. L'oggetto e l'ambito di applicazione	»	39
1.2. Le novità in sintesi	»	40
2. Il concetto di accountability e il suo ruolo nel GDPR	»	41
3. Il consenso al trattamento dei dati	»	46
4. L'informativa del trattamento dei dati ai sensi dell'art. 13 GDPR	»	47
5. L'RPD – Responsabile per la protezione dei dati personali	»	50
5.1. I compiti	»	51
5.2. La designazione di un unico RPD per conto di più soggetti pubblici	»	60
5.3. Obbligatorietà della designazione del RPD	»	61
5.4. Le qualità professionali e il possesso titoli	»	64

5.5. Le questioni attinenti alla designazione di un responsabile della protezione dei dati esterno	»	66
5.6. La pluralità di enti pubblici per conto dei quali viene svolto l'incarico e la pluralità di servizi forniti anche al medesimo titolare	»	69
5.7. L'individuazione, all'interno del RPD persona giuridica, del referente persona fisica	»	70
5.8. La durata dell'incarico	»	72
5.9. Il coinvolgimento da parte del titolare e lo svolgimento dei compiti da parte del RPD	»	73
5.10. Le risorse messe a disposizione dal titolare e la costituzione di un gruppo di collaboratori (team) del RPD	»	78
5.11. L'incompatibilità con altri incarichi e il conflitto di interessi	»	79
5.12. L'RPD esterno che fornisce servizi IT quale responsabile del trattamento	»	83
6. La valutazione di impatto: l'art. 35	»	86
6.1. Quando la DPIA è obbligatoria?	»	88
7. La violazione dei dati personali: <i>data breach</i>	»	89
8. La certificazione e i codici di condotta: gli artt. 40 e 42 e ss.	»	89
9. Il responsabile del trattamento dei dati: l'art. 28	»	96
10. La responsabilità e le sanzioni del regolamento Europeo: gli artt. 77 e ss.	»	99
10.1. Le sanzioni del regolamento Europeo	»	104
 CAPITOLO 4		
IL D.LGS. DEL 2018, N. 101: UNA SINTESI DEI CONTENUTI	»	109
1. L'ambito di applicabilità: art. 2, comma 1, lett. c)	»	110
2. I trattamenti collegati ad un interesse pubblico: art. 2, comma 1, lett. f)	»	110
3. I dati genetici, biometrici e sulla salute ed utilizzo dei dati biometrici dei soggetti autorizzati: art. 2, comma 1, lett. f)	»	111
4. I dati relativi a condanne penali e reati: art. 2, comma 1, lett. f)	»	112
5. I casi di restrizione dei diritti dell'interessato: art. 2, comma 1, lett. f)	»	112
6. I diritti riguardanti le persone decedute: art. 2, comma 1, lett. f)	»	113
7. I soggetti autorizzati e designati art. 2, comma 1, lett. f)	»	113
8. L'organismo nazionale di accreditamento: art. 2, comma 1, lett. f)	»	113
9. Le disposizioni in settori specifici – rapporto di lavoro: art. 9, comma 1	»	114
10. Il rafforzamento del ruolo del garante: artt. 2, comma 1, lett. f) e 14, comma 1	»	115

11. Le funzioni di accertamento e ispettive del Garante: art. 14, comma 1, lett. <i>b</i> )	»	115
12. Le funzioni sanzionatorie: art. 15	»	116
CAPITOLO 5		
ALCUNI DELITTI IN MATERIA DI TRATTAMENTO E ACCESSO ABUSIVO AI DATI E ALLE INFORMAZIONI	»	117
1. Il concetto di domicilio informatico e l'accesso abusivo	»	117
2. Il trattamento illecito dei dati personali: artt. 167, 167- <i>bis</i> e 167- <i>ter</i> c.p. modificati e introdotti dal d.lgs. n. 101 del 2018	»	125
3. La detenzione e la diffusione di virus	»	131
4. Il danneggiamento informatico	»	137
4.1. L'art. 635- <i>bis</i> c.p. – Danneggiamento di informazioni, dati e programmi informatici. L'aggravante dell'operatore di sistema	»	145
4.2. Art. 635- <i>ter</i> c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	»	148
4.3. Art. 635- <i>quater</i> c.p. – Danneggiamento di sistemi informatici o telematici	»	150
4.4. Art. 635- <i>quinquies</i> c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità	»	151
5. L'intercettazione illecita	»	153
6. La violazione dei segreti	»	154
7. La violazione della corrispondenza	»	157
CAPITOLO 6		
GLI ELEMENTI DI BASE DELLE INFORMAZIONI E DELL'INFORMATICA: CENNI TECNICI	»	163
1. L'era digitale	»	163
2. Il sistema binario	»	163
3. Bit, MegaByte, GigaByte, TeraByte	»	164
4. Il personal computer e lo smartphone: come sono fatti. Le applicazioni»	»	167
4.1. Le reti informatiche	»	172
5. Il web: come funziona Internet?	»	174
6. Cos'è un IP?	»	176
7. I concetti di sicurezza	»	179
7.1. I virus malware	»	184
7.2. I firewall	»	188
7.3. Il Backup, il ripristino e il recupero dati	»	190
7.4. Il cloud	»	191

7.5. Il cloud forensics e le nuove frontiere delle indagini informatiche nel processo penale	»	194
7.6. La crittografia dei dati e la steganografia	»	199
7.7. Il social engineering e il suo utilizzo anche in campo informatico	»	202
CAPITOLO 7		
LA CYBERSECURITY: LA SICUREZZA CIBERNETICA NAZIONALE	»	207
1. Il Perimetro di Sicurezza Nazionale Cibernetica: le caratteristiche dello spazio cibernetico e l'analisi della minaccia Cyber	»	208
1.1. Il dominio cibernetico	»	208
1.2. L'analisi della minaccia cibernetica	»	210
1.3. Le relazioni presentate al Parlamento sulla politica dell'informazione per la sicurezza	»	212
1.4. Le diverse tipologie di attacco	»	214
1.5. La Cyber war e la minaccia cibernetica militare	»	215
1.6. Alcune problematiche connesse alla Cyber war	»	216
1.7. Il Cyber crime, la Cyber intelligence e il Cyber terrorismo	»	218
2. La normativa nazionale per la sicurezza e la difesa cibernetica	»	222
2.1. Premessa	»	222
2.2. L'evoluzione della normativa nazionale in materia di sicurezza cibernetica	»	223
2.3. Il decreto legge del 2019, n. 105 sul perimetro di sicurezza nazionale cibernetica	»	230
2.4. La nascita dell'Agenzia Nazionale di Cybersecurity. Il decreto legge del 2021 n. 82	»	234
2.5. La notifica degli incidenti aventi impatto su beni ICT	»	246
3. Il contrasto della criminalità informatica e la tutela dei diritti nel dominio cibernetico	»	249
3.1. L'elaborazione a livello sovranazionale e la Convenzione del Consiglio d'Europa sui crimini informatici (c.d. Convenzione di Budapest	»	249
3.1.1. Gli interventi di diritto penale sostanziale	»	251
4. La difesa cibernetica: il quadro attuale e i progetti di rafforzamento	»	255
4.1. Le operazioni Cyber della difesa	»	255
4.2. Il comando interforze per le operazioni cibernetiche e le computer network operations	»	257
4.3. Le linee di sviluppo della difesa cibernetica	»	260
5. L'amministrazione digitale e la sicurezza dei dati	»	262

5.1. Il processo di digitalizzazione delle pubbliche amministrazioni »	262
5.2. La sicurezza informatica nel sistema informativo della P.A. »	265
5.3. La sicurezza informatica e il Piano triennale 2019-2021 »	267
6. La sicurezza delle reti e la tecnologia 5G »	271
6. 1. La tecnologia 5G »	272
7. Protezione della filiera industriale automatizzata e interconnessa (progetto industria 4.0) »	276
7.1. Le soluzioni tecnologiche individuate dalla logica Industria 4.0 »	278
7.2. La Cybersecurity e l'industria 4.0 »	279
8. L'approccio UE all'azione di contrasto al Cybercrime »	281
8.1. Le minacce alle reti e ai sistemi informatici europei »	281
8.2. La Cybersicurezza e 5G »	282
9. La sicurezza informatica Intelligente »	284

## CAPITOLO 8

### LE NUOVE FRONTIERE DELL'INNOVAZIONE E DELLA SICUREZZA. I BIG DATA, LE MACCHINE PREDITTIVE, L'INTELLIGENZA ARTIFICIALE E LA ROBOTICA

»	287
1. I Big Data »	289
1.1. La filiera dei Big Data »	290
1.2. Il ciclo dei Big Data: dalla raccolta all'elaborazione »	293
1.3. L'interpretazione e l'utilizzo dei Big Data »	301
1.4. I Big Data e lo sviluppo di reti e servizi innovativi (5G, IoT, M2M, IA) »	306
2. L'Internet Of Things e gli Smart Assistant »	309
2.1. Gli Smart Assistant: assistenti o spie? »	313
3. L'Intelligenza Artificiale, Deep Learning e Machine Learning »	316
3.1. I profili di compatibilità e di responsabilità degli agenti non umani »	319
3.2. L'IA e il diritto »	327
3.3. L'Intelligenza Artificiale: le opportunità e i rischi etico-sociali »	331
3.4. L'Intelligenza Artificiale e il GDPR »	335
3.5. Osservazioni etiche »	345
4. L'arrivo dei robot e dell'uomo che diventa macchina »	354

CAPITOLO 9	
IL CONTROLLO TECNOLOGICO A DISTANZA DEI LAVORATORI NEL MONDO DIGITALE E NELL'ERA DEL LAVORO AGILE: LA RIFORMA DELL'ART. 4 DELLO STATUTO DEI LAVORATORI	» 361
1. Breve introduzione	» 361
1.1. Alcuni cenni storici: dall'OCSE al GDPR	» 363
2. L'art. 4 ante e post-riforma	» 365
3. La normativa sui controlli a distanza nel Codice privacy e nel regolamento Europeo del 2016, n. 679	» 369
4. Gli strumenti tecnologici di controllo diretto e indiretto: questioni giuridiche e giurisprudenziali	» 371
4.1. I provvedimenti dell'Autorità Garante	» 378
CONCLUSIONI	» 387
BIBLIOGRAFIA	» 389
SITOGRAFIA	» 395