

INDICE

Cybersecurity: una sfida per tutti di Giuseppe Busia p.	IX
I. La disciplina della cybersecurity nell'Unione Europea »	1
Alfonso Contaldo - Luca Salandri	
1. Cenni per una sommaria definizione di cybersecurity e di cyberdefence. . . »	1
1.1. L'implementazione in ambito dell'UE delle policies in materia di <i>cybersecurity</i> »	7
2. Le policies del Consiglio europeo della UE in materia di cybersicurezza, di ciberresilienza e di diplomazia cibernetica »	11
2.1. Le Conclusioni del Consiglio europeo della UE più significative in materia »	19
2.2. La peculiarità della Comunicazione congiunta del Consiglio UE n. 14435/17 del 20 novembre 2017 e del Progetto di conclusioni della Commissione sulla comunicazione congiunta al Parlamento europeo e al Consiglio " <i>Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE</i> " »	24
3. La disciplina giuridica del settore a seguito della direttiva comunitaria in materia di protezione delle infrastrutture critiche »	32
4. La cybersicurezza e le previsioni del Regolamento comunitario cd. EIDAS (<i>Electronic Identification Authentication and Signature</i>) »	36
5. La prescrizioni in tema di cybersicurezza a seguito della Direttiva NIS . . . »	41
6. Ulteriori previsioni della Direttiva NIS »	53
II. Il Cybersecurity Act »	57
Flavio Campara	
Premesse »	57
1. Il <i>Cybersecurity Act</i> : lo scenario e le ragioni dell'intervento. »	59
2. Il CSA: struttura e ambito definitorio »	66
3. L'ENISA: una "nuova" agenzia dell'Unione europea per la cybersicurezza . »	71
4. Il CSA, parte I: la normativa sull'ENISA »	74
4.1. Mandato, compiti ed obiettivi. »	74
4.2. L'organizzazione dell' ENISA »	85
5. Il CSA, parte II: la certificazione della cybersicurezza »	92
5.1. La <i>ratio</i> di un quadro europeo di certificazione della <i>cybersecurity</i> . . »	92
5.2. Il sistema europeo di certificazione della cybersicurezza »	95

III. La disciplina italiana in tema di cybersecurity »	119
Flaviano Peluso	
1. Gli indirizzi per la protezione cibernetica e la sicurezza informatica »	119
2. Il Piano nazionale per la protezione cibernetica e la sicurezza informatica . »	124
3. Il d. lgs. 18 maggio 2018 n. 65: attuazione della delega nella legge n. 163 del 2017. »	126
3.1. Il ruolo dei CSIRT e la gestione degli incidenti alla luce del d. lgs. n. 65/2018 »	130
3.2. Gli obblighi degli operatori in caso di incidenti alla luce del d. lgs. n. 65/2018 »	136
4. Le regole tecniche del CAD e la loro applicabilità alla sicurezza informatica: brevi analisi »	138
IV. Protezione dei dati personali e cybersecurity »	145
Davide Mula	
1. Privacy, Data Protection e Cybersecurity »	145
2. Direttiva NIS, Regolamento ENISA e impatto sulla disciplina in materia di trattamento dei dati personali »	149
3. Rapporto tra misure di <i>cybersecurity</i> e misure di sicurezza in materia di trattamento dei dati personali »	154
4. Misurazione del rischio <i>privacy</i> »	159
5. Incidenti e violazioni dei dati »	163
6. <i>Data security</i> e <i>cybersecurity</i> dei servizi <i>cloud</i> »	167
7. Conclusioni: <i>cybersecurity</i> e <i>accountability</i> »	173
V. La disciplina della sicurezza del perimetro cibernetico nazionale anche alla luce dello standard 5G »	177
Alfonso Contaldo	
1. Le norme internazionali ed europee sul 5G nello Spettro radio: cenni. »	177
2. La disciplina italiana sul 5G nello Spettro radio »	184
2.1. L'estensione al 5G delle competenze del cd. <i>golden power</i> »	185
2.2. L'integrità e la sicurezza delle reti 5G e gli obiettivi della cd. <i>golden power</i> »	198
3. La delineazione del perimetro cibernetico nazionale alla luce del 5G »	201
3.1. Le procedura di notifica di incidenti informatici impattanti sul perimetro cibernetico. »	205
3.2. Le procedure di notifica riguardo le forniture di beni e servizi ICT necessari alle reti strategiche »	207
4. I soggetti vigilanti: il Centro Valutazione e Certificazione Nazionale ed il MISE»	212

4.1. I compiti della Presidenza del Consiglio »	215
5. Le sanzioni amministrative e penali a seguito di lesioni (anche potenziali) del perimetro cibernetico »	216
VI. It & Cybersecurity Standards »	221
Luca Salandri	
1. Premesse necessarie »	221
2. Norme tecniche e competitività nella globalizzazione produttiva »	226
3. L'importanza dell'implementazione della sicurezza informativa nell'automazione industriale »	235
4. L'importanza in Europa dell'Organizzazione internazionale per la normazione»	249
5. L'importanza della standardizzazione negli USA »	302
Bibliografia »	317