

INDICE

<i>Introduzione</i>	V
<i>Introduction</i>	IX

PARTE I

CAPITOLO I

DARE REGOLE ALLE TECNOLOGIE

di *Andrea Rossetti*

1. Il linguaggio del diritto	I
1.1. Il linguaggio del diritto e le sue metafore	I
1.2. Regole tecnologiche e regole tecnomomiche	3
2. Regolamentare le tecnologie	4
2.1. Occorre regolare le tecnologie?	4
2.2. Come regolare le tecnologie	5
2.3. Architettura delle regole	6
2.4. Regole tecnomomiche e pragmatica della tecnologia	7
2.5. Un approccio interdisciplinare alla regolazione delle tecnologie	8
3. L'attività del nomografo nella regolamentazione delle nuove tecnologie	9
3.1. La Soft Law	9
3.2. Approccio basato sul rischio	10
3.3. L'ecosistema normativo	11
3.4. Le fondamenta delle norme giuridiche	12
4. La tecnologia come legislazione	13

CAPITOLO II

DATA PROTECTION

di *Stefano Ricci*

1. Privacy e <i>data protection</i> nella società dell'informazione	15
---	----

2.	Le regole della <i>data protection</i> (e della <i>data governance</i>)	19
3.	Origine storica del diritto alla riservatezza e del diritto alla protezione dei dati personali	23
4.	<i>Privacy Invading Technologies</i> (PITs) e <i>Privacy Enhancing Technologies</i> (PETs)	34

CAPITOLO III

DATA SECURITY: LE NORMATIVE SULLA SICUREZZA DI SISTEMI INFORMATIVI, RETI E DATIdi *Andrea Palumbo*

1.	Introduzione	41
2.	Classificazione delle differenti normative	43
3.	Evoluzione storica della normativa per la sicurezza di sistemi informativi, reti e dati	44
4.	I principi comuni alle normative in materia di sistemi informativi, reti e dati dell'Unione Europea	46
5.	L'approccio basato sul rischio	47
6.	La <i>Soft-law</i> quale strumento integrativo dei principi in materia di sicurezza	50
7.	Le misure di sicurezza	51
8.	Gli obiettivi di sicurezza	52
9.	La gestione degli incidenti informatici	53
10.	Le normative più rilevanti in materia di sistemi informativi, reti e dati nell'Unione Europea	56

CAPITOLO IV

REGOLE PER L'INTELLIGENZA ARTIFICIALEdi *Federico Cabitza, Andrea Rossetti*

1.	ClipSapiens	61
2.	Come funziona l'AI	62

3.	Modelli di regolamentazione	64
4.	Il regolamento europeo sull'intelligenza artificiale	66
4.1.	Le pratiche proibite	67
4.2.	Le pratiche ad alto rischio	68
5.	Sistemi a rischio nullo o limitato	69

CAPITOLO V

REGOLE PER I SERVIZI DIGITALI

di *Alessandro Malinconico*

1.	Premessa	71
2.	Il sottile confine tra digitale e fisico	76
3.	La Direttiva sui contenuti e servizi digitali e i suoi effetti dirompenti	78
4.	Il Regolamento sui servizi digitali e l'importanza dei servizi intermediari	86

CAPITOLO VI

IDENTITÀ, DOCUMENTO E FIRMA NEL CONTESTO DELLA SOCIETÀ DELL'INFORMAZIONE

di *Andrea Rossetti*

1.	Identità digitale	99
2.	Il regolamento sull'identificazione elettronica e i servizi fiduciari	100
3.	Il documento informatico	101
3.1.	La definizione di documento digitale	101
3.1.1.	Che cosa è un documento giuridico	101
3.1.2.	Caratteristiche del documento informatico	103
3.2.	Il quadro normativo di riferimento	105
4.	I sistemi di firma	106
4.1.	La chiave asimmetrica	106
4.2.	Le firme elettroniche	108
5.	Copie e duplicati	111
6.	Posta elettronica certificata	112

CAPITOLO VII

COMPLIANCE E CONTRASTO DELLE ATTIVITÀ ILLECITEdi *Serena Sardano*

1.	Premessa	115
2.	Il modello di organizzazione e gestione previsto dal d.lgs. n. 231/2001	117
3.	I reati informatici: panoramica generale	119
4.	Le attività di controllo per la prevenzione dei reati informatici previsti dal d.lgs. n. 231/2001	122
5.	I reati informatici ricompresi nel catalogo dei reati presupposto di cui al d.lgs. n. 231/2001	124
5.1.	Frode informatica (art. 640-ter c.p.)	124
5.2.	Falsità riguardanti un documento informatico (art. 491-ter c.p.)	125
5.3.	L'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	126
5.4.	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615- <i>quater</i> c.p.) e Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- <i>quinquies</i> c.p.)	127
5.5.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617- <i>quater</i> c.p.) e Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617- <i>quinquies</i> c.p.)	128
5.6.	Danneggiamento di informazioni, dati e programmi informatici (art. 635-ter c.p.) e Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)	129
5.7.	Danneggiamento di sistemi informatici o telematici (art. 635- <i>quater</i> c.p.) e Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- <i>quinquies</i> c.p.)	130

5.8. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640- <i>quinquies</i> c.p.)	131
5.9. Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. I, comma II, d.l. n. 105 del 21 ottobre 2019)	131
6. La compliance e il contrasto alle attività illecite in ambito privacy	131
7. Diffamazione a mezzo stampa telematica e rapporti con la <i>compliance</i>	133

PART II

CHAPTER I

GIVING RULES TO TECHNOLOGIES

by *Andrea Rossetti*

1. The language of law	137
1.1. The language of law and its metaphors	137
1.2. Technological rules and technonomic rules	138
2. Regulating technologies	140
2.1. Should technologies be regulated?	140
2.2. How to regulate technologies	140
2.3. Architecture of rules	142
2.4. Technological rules and pragmatics of technology	142
2.5. An interdisciplinary approach to technology regulation	143
3. The work of the nomographer in the regulation of new technologies	144
3.1. The Soft Law	144
3.2. Risk-based approach	145
3.3. The Regulatory Ecosystem	146
3.4. The foundations of legal norms	147
4. Technology as legislation	148

CHAPTER II

DATA PROTECTION

by *Stefano Ricci*

1. Privacy and <i>data protection</i> in the information society	151
--	-----

2.	The rules of <i>data protection</i> (and <i>data governance</i>)	155
3.	Historical origin of the right to privacy and the right to protection of personal data	159
4.	<i>Privacy Invading Technologies</i> (PITs) and <i>Privacy Enhancing Technologies</i> (PETs)	169

CHAPTER III

INFORMATION SYSTEM, NETWORK AND DATA SECURITY REGULATIONSby *Andrea Palumbo*

1.	Introduction	177
2.	Classification of different regulations	179
3.	Historical development of legislation for the security of information systems, networks and data	180
4.	The principles common to the European Union's information systems, networks and data regulations	182
5.	The risk-based approach	183
6.	<i>Soft-law</i> as a supplementary instrument to security principles	186
7.	Security Measures	187
8.	Security Targets	188
9.	Computer Incident Management	189
10.	The most relevant regulations on information systems, networks and data in the European Union	192

CHAPTER IV

RULES FOR ARTIFICIAL INTELLIGENCEby *Federico Cabitza, Andrea Rossetti*

1.	ClipSapiens	195
2.	How AI works	196
3.	Regulatory models	197
4.	The European Artificial Intelligence Regulation	200
4.1.	Prohibited practices	201

4.2. High-risk practices	201
5. Systems with no or limited risk	202

CHAPTER V

DIGITAL SERVICESby *Alessandro Malinconico*

1. Introduction	205
2. The fine line between digital and physical	210
3. The Digital Content and Services Directive and its disruptive effects	212
4. The Digital Services Act and the importance of intermediary services	219

CHAPTER VI

IDENTITY, DOCUMENT AND SIGNATURE IN THE CONTEXT OF THE INFORMATION SOCIETYby *Andrea Rossetti*

1. Digital identity	231
2. The Regulation on Electronic Identification and Trust Services	232
3. The digital document	233
3.1. The definition of a digital document	233
3.1.1. What is a legal document	233
3.1.2. Characteristics of the digital document	235
3.2. The regulatory framework	237
4. Signature systems	238
4.1. The Asymmetric Key	238
4.2. Electronic signatures	240
5. Copies and duplicates	242
6. Certified electronic mail	244

CHAPTER VII

COMPLIANCE AND LAW ENFORCEMENTby *Serena Sardano*

1. Foreword	248
-----------------------	-----

2.	The organisation and management program provided for by Legislative Decree No. 231/2001	249
3.	Computer crimes: general overview	251
4.	Control activities for the prevention of computer crimes under Legislative Decree No. 231/2001	254
5.	Computer offences included in the catalogue of predicate offences under Legislative Decree No. 231/2001	256
5.1.	Computer fraud (Article 640-ter of the Criminal Code)	256
5.2.	Forgery of a computer document (Article 491-ter of the Criminal Code)	257
5.3.	Unauthorised access to a computer or telecommunications system (Article 615-ter of the Criminal Code)	258
5.4.	Possession, dissemination and unauthorised installation of equipment, codes and other means of accessing computer or telecommunications systems (Article 615-quater of the Criminal Code) and Dissemination of computer equipment, devices or programmes aimed at damaging or interrupting a computer or telecommunications system (Article 615-quinquies of the Criminal Code)	259
5.5.	Illegal interception, obstruction or interruption of computer or telematic communications (Article 617-quater of the Criminal Code) and Illegal possession, dissemination and installation of equipment and other means designed to intercept, obstruct or interrupt computer or telematic communications (Article 617-quinquies of the Criminal Code)	260
5.6.	Damage to computer information, data and programmes (Article 635-ter of the Criminal Code) and Damage to computer information, data and programmes used by the State or other public body or in any case of public utility (Article 635-ter of the Criminal Code)	261
5.7.	Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code) and damaging computer and telecommunication systems of public utility (Article 635-quinquies of the Criminal Code)	262

5.8.	Computer fraud by the person providing electronic signature certification services (Article 640- <i>quinquies</i> of the Criminal Code)	263
5.9.	Violation of the National Cybersecurity Perimeter (Art. 1, para. 11, Decree-Law No. 105 of 21 October 2019)	263
6.	<i>Compliance</i> and the fight against unlawful privacy activities	264
7.	Telematic defamation and relations with <i>compliance</i>	266

