

# Indice

*pag.*

## Capitolo I

### **Introduzione alla regolazione europea della società digitale**

di *Franco Pizzetti*

1.	Contenuto del Volume	1
2.	Connessione tra regolazione e interoperabilità delle strutture fisiche di telecomunicazione	3
3.	Il rafforzamento del ruolo della Commissione e l'espansione normativa dell'UE a livello globale	4
4.	Lo sforzo regolatorio dell'UE e il suo rafforzamento come potere digitale globale	6

## Capitolo II

### **Le fonti del diritto dell'Unione europea per la disciplina della società digitale**

di *Antonio Iannuzzi*

1.	La disciplina europea della società digitale: il quadro politico-normativo di riferimento	9
2.	Il recupero della centralità delle fonti del diritto e la pretesa di regolare la tecnologia come affermazione della sovranità digitale europea	13
3.	La centralità del regolamento europeo come fonte privilegiata per il governo della società digitale: vantaggi e problemi	19
4.	I principi "para-costituzionali" della società digitale	23
5.	Il ricorso alle norme armonizzate come paradigma normativo ricorrente per la disciplina delle tecnologie digitali	31
6.	Le norme armonizzate nel quadro normativo vigente risultante dal Regolamento UE n. 1025/2012	37
7.	Il vantaggio e le prospettive della standardizzazione tecnica europea	46

### Capitolo III

## La disciplina del “rischio digitale”

di *Erik Longo*

1.	Introduzione	53
2.	Gli sviluppi recenti nelle scienze sociali e la regolazione del rischio	56
3.	L'emergere del “rischio digitale”	59
4.	<i>La digital risk society</i>	61
4.1.	L'ambivalenza delle componenti negative e positive dei rischi digitali	64
4.2.	Rischi prodotti e ricercati attraverso dispositivi tecnologici	65
4.3.	Gestire il rischio digitale	68
5.	Il rischio digitale nella normativa europea più recente	71
5.1.	L'approccio basato sul rischio nella regolazione dell'Intelligenza Artificiale: l' <i>Artificial Intelligence Act</i>	72
5.2.	Il rischio come giustificazione e oggetto della regolazione: il <i>Digital Services Act</i>	75
5.3.	Organizzazioni e procedure per regolare il rischio cyber: la Direttiva <i>NIS 2</i> e il <i>Cybersecurity Act</i>	77
5.4.	Gli strumenti di gestione del rischio usati per determinare il livello di conformità: il <i>General Data Protection Regulation</i>	79
6.	Conclusioni	81

### Capitolo IV

## Autorità indipendenti e di governo della società digitale

di *Simone Calzolaio*

1.	Introduzione, oggetto, limiti del contributo	83
2.	Il livello europeo: una proposta di tripartizione descrittiva	85
2.1.	Autorità indipendente e di governo: il CEPD	87
2.2.	Autorità indipendente, non di governo: ENISA	90
2.3.	Autorità di governo, non indipendente: la Commissione UE dall'agenda alla bussola digitale e al NGEU	93
4.	Alcune prime considerazioni di sintesi	99
5.	Il livello nazionale. Autorità indipendente e di governo: il GPDP	100
5.1.	Autorità di governo, non indipendente: l'Agid, l'ACN	100
5.2.	<i>Segue</i> : L'attuazione del PNRR come leva per l'accentramento di funzioni in capo alla Presidenza del Consiglio	102
5.3.	Altre autorità (AGCOM, AGCM) e materie orfane (IA)	104
6.	Funzioni e interrelazioni fra Autorità della società digitale. Indizi per un modello di <i>governance europea dei dati</i> ?	105

## Capitolo V

### I regolamenti intersettoriali per l'istituzione dei «data spaces»: *Data Governance Act* e *Data Act*

di Antonio Iannuzzi

1. Gli obiettivi	107
2. Dal Regolamento generale sulla protezione dei dati personali al <i>Data Governance Act</i>	108
3. Le definizioni di «dati» e di «governance dei dati»	111
4. Il riuso dei dati detenuti da soggetti pubblici	113
5. Il ruolo dei fornitori di servizi di intermediazione dei dati ( <i>data sharing</i> )	116
6. L'altruismo dei dati	119
7. Il Comitato europeo per l'innovazione in materia di dati	121
8. Gli aspetti pubblicistici del <i>Data Act</i>	123
9. Dai regolamenti per l'istituzione dei <i>data spaces</i> all' <i>Artificial Intelligence Act</i>	129

## Capitolo VI

### Il *Digital Service Act* tra continuità (solo apparente) ed innovazione

di Marco Orofino

1. Introduzione	134
2. L'ambito di applicazione materiale	136
3. L'ambito di applicazione territoriale	137
4. L'armonizzazione delle norme sulle esenzioni di responsabilità dei prestatori di servizi intermediari	138
4.1. I prestatori di servizi di intermediazione c.d. <i>mere conduit</i>	139
4.2. I prestatori di servizi intermediari c.d. <i>caching</i>	140
4.3. I prestatori di servizi intermediari c.d. <i>hosting</i>	140
5. Una prima armonizzazione degli ordini emessi dalle autorità giudiziarie o amministrative a carico dei prestatori di servizi di intermediazione	142
6. Gli obblighi in materia di dovere di diligenza (c.d. <i>due diligence</i> )	143
6.1. Gli obblighi a carico di tutti i prestatori di servizi intermediari	144
6.2. Gli obblighi aggiuntivi per i prestatori di servizi di memorizzazione, comprese le piattaforme online	146
6.2.1. L'implementazione di un meccanismo di <i>notice</i>	146
6.2.2. L'obbligo di motivazione delle restrizioni imposte	147

	<i>pag.</i>
6.2.3. La notifica di sospetti di reati	147
6.3. Le disposizioni aggiuntive per i fornitori di piattaforme online	148
6.3.1. Il sistema interno di gestione dei reclami	148
6.3.2. La risoluzione extragiudiziale delle controversie	149
6.3.3. I c.d. segnalatori attendibili	150
6.3.4. Misure e protezione contro gli abusi	150
6.3.5. Obblighi di comunicazione trasparente aggiuntivi per i fornitori di piattaforme online	151
6.3.6. Progettazione e organizzazione delle interfacce online (c.d. <i>due diligence by design</i> )	152
6.3.7. Pubblicità sulle piattaforme	152
6.3.8. Trasparenza sui sistemi di raccomandazione	153
6.3.9. Obblighi specifici di protezione dei minori	154
6.4. Le disposizioni aggiuntive a carico dei fornitori di piattaforme online che consentono la conclusione di contratti a distanza	154
6.4.1. L'obbligo di tracciabilità degli operatori commerciali	155
6.4.2. L'obbligo di rendere le interfacce conformi <i>by design</i> a determinate prescrizioni	155
6.4.3. Obbligo di informazione riguardo a prodotti o servizi illegalmente offerti	156
6.5. Gli obblighi supplementari a carico di piattaforme online e motori di ricerca molto grandi	156
6.5.1. L'obbligo di valutazione dei rischi sistemici	158
6.5.2. L'obbligo di attenuazione del rischio	159
6.5.3. Il meccanismo di risposta alle crisi	159
6.5.4. Gli ulteriori obblighi in materia di sistemi di raccomandazione e di trasparenza della pubblicità online	160
6.5.5. L'obbligo di istituire una funzione aziendale di controllo della conformità	161
6.5.6. L'obbligo di sottoporsi a revisioni indipendenti	162
6.5.7. L'obbligo di consentire l'accesso ai propri dati	162
6.5.8. L'obbligo di contribuire all'attività di vigilanza e gli altri obblighi imponibili dalla Commissione europea	163
6.6. Il ruolo dei codici di condotta	163
7. La <i>governance</i> del DSA	164
7.1. La designazione delle autorità competenti e l'individuazione del coordinatore dei servizi digitali	165
7.2. Le prescrizioni relative al Coordinatore dei servizi digitali ed i suoi poteri	165
7.3. Il Comitato europeo per i servizi digitali	167
7.4. Il ruolo della Commissione europea	168
7.5. I meccanismi di coerenza	169

	<i>pag.</i>
7.6. Le sanzioni pecuniarie	169
8. Osservazioni conclusive	170

## Capitolo VII

### **Il *Digital Market Act*: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust**

di *Marco Orofino*

1. Premessa	175
2. L'ambito di applicazione materiale del <i>Digital Market Act</i>	177
3. L'ambito di applicazione territoriale	178
4. Il processo di designazione dei c.d. <i>gatekeeper</i>	178
4.1. Il primo round di designazione	181
5. La natura degli obblighi regolamentari imposti ai <i>gatekeeper</i>	182
6. Gli obblighi comportamentali c.d. <i>Don'ts</i> e <i>Dos!</i>	185
6.1. I divieti ( <i>Don'ts</i> )	185
6.2. Gli obblighi ( <i>Dos!</i> )	188
7. La funzione indipendente di controllo della conformità	192
8. La <i>governance</i> del DMA e il ruolo della Commissione europea	193
9. I compiti specifici attribuiti alla Commissione europea	195
9.1. L'atto di esecuzione della Commissione relativa all'inosservanza degli obblighi imposti ai <i>gatekeeper</i>	196
9.2. Il contenuto dell'atto di esecuzione: l'eventualità dell'ammenda	196
10. Osservazioni conclusive	198

## Capitolo VIII

### **La disciplina della *cybersecurity* nell'Unione europea e in Italia**

di *Erik Longo*

1. Introduzione	203
2. Il cyberspazio	205
3. Le trasformazioni della cybersicurezza	206
4. Regole e politiche a livello europeo sulla <i>cybersecurity</i>	208
4.1. La disciplina prima del 2013	209
4.2. Le Strategie europee sulla <i>cybersecurity</i>	212
4.3. Il nesso tra <i>cybersecurity</i> e protezione dei dati	215

	<i>pag.</i>
4.4. La Direttiva NIS	216
4.5. La Direttiva NIS 2	219
4.6. Gli altri provvedimenti dell'UE	223
5. L'attuazione della NIS in Italia	224
6. L'avvio del processo di attuazione della NIS 2 in Italia	228
7. Conclusioni	231
 <i>Gli autori</i>	 235