

SOMMARIO

INTRODUZIONE	9
CAPITOLO 1 · DALLA GLOBALIZZAZIONE ALLA “DIMENSIONE DIGITALE”	13
1.1 Le 3 Dimensioni della vita moderna	15
1.2 Gli effetti sulla società	20
1.3 I punti di forza e le opportunità	23
1.4 I punti di debolezza e le minacce	24
1.5 La responsabilità politico-istituzionale	25
1.6 I diritti delle persone	28
1.6.1 <i>La sfera della vita privata</i>	30
1.6.2 <i>Il Digital Divide</i>	32
CAPITOLO 2 · DALL’ICT AL DIRITTO: L’INFORMATICA GIURIDICA	35
2.1 L’Ontologia dell’ICT	35
2.2 L’Informatica giuridica	38
2.3 Legal Informatics: perimetro e definizione	41
CAPITOLO 3 · IL CITTADINO E L’E-GOVERNMENT	49
3.1 La posta elettronica certificata	52
3.2 Il domicilio digitale	57
3.2.1 <i>Il valore della notificazione nella dimensione digitale</i>	61
3.3 La firma digitale	62
3.4 L’e-invoking	64
3.5 L’identità digitale	68

CAPITOLO 4 · IL CYBERSPACE	75
4.1 Introduzione	75
4.2 Dall'E-commerce al Social Commerce	78
4.3 Il “contratto” nella dimensione digitale	83
4.3.1 <i>I contratti informatici, telematici e gli smart contract</i>	88
4.4 L'asimmetria informativa	94
4.5 L'evoluzione dei sistemi di pagamento nella dimensione digitale	102
4.6 Le cybercurrencies e le criptovalute	104
4.7 I beni intangibili della dimensione digitale	111
4.7.1 <i>I Non-Fungible-Token (NFT)</i>	111
4.7.2 <i>La Cassazione: i “beni intangibili” sono cose mobili</i>	113
4.7.3 <i>Il dato come “asset patrimoniale”</i>	119
4.8 Le Smart Cities e le Smart Communities	125
CAPITOLO 5 · L'ARTIFICIAL INTELLIGENCE ED IL MACHINE LEARNING	133
5.1 La Human e l'Artificial Intelligence (AI)	133
5.2 La nascita dell'Artificial Intelligence	138
5.3 Gli algoritmi nel contesto giuridico	140
5.4 Il “dato” nella moderna società	143
5.5 Il Machine Learning (ML)	146
5.6 I Dati sintetici: l'ultima frontiera della data protection	150
CAPITOLO 6 · IL CYBERCRIME	157
6.1 I reati informatici	163
6.2 Reati informatici e reati connessi ai sistemi informatici	164
6.3 I reati informatico-sociali ed a sfondo sessuale	166
6.3.1 <i>Il cyberstalking ed il cyberharassment</i>	169
6.3.2 <i>Il cyberbullismo</i>	172
6.3.3 <i>Il sexting</i>	179
6.3.4 <i>La revenge pornography</i>	181
6.3.5 <i>La sextortion</i>	182
6.4 I reati informatico-economici	183
6.4.1 <i>L'e-commerce e la contraffazione</i>	183
6.4.2 <i>La digital piracy</i>	187
6.4.3 <i>Il contrasto alla e-contraffazione</i>	188
6.5 Il contrasto ai cybercrime e la giurisdizione	190

CAPITOLO 7 · MODALITÀ E TECNICHE INFORMATICHE
DEL CYBERCRIME

197

CAPITOLO 8 · REGOLAMENTO GENERALE SULLA
PROTEZIONE DEI DATI

	211
8.1 Introduzione	211
8.2 Definizioni	214
8.3 La protezione nel trattamento dei dati personali	218
8.4 Il General Data Protection Regulation	225
8.4.1 <i>GDPR: innovazioni e pilastri</i>	228
8.5 La nuova doppia giurisdizione e la prospettiva etica	230
8.6 In “linea di principio”	243
8.7 GDPR: alcune considerazioni sulla privacy nel C2G	253
8.8 Gli obblighi previsti dal GDPR	255
8.9 L’informativa	256
8.10 Il consenso	259
8.10.1 <i>Le deroghe al consenso</i>	262
8.11 Gli aspetti organizzativi	264
8.12 L’accountability (responsabilizzazione)	265
8.13 Il Privacy Impact Assessment	267
8.14 Il registro delle attività di trattamento	267
8.15 La gestione dei data breach	268
8.15.1 <i>L’Holistic Complexity e la Cyber Resilience</i>	270
8.16 Gli attori del trattamento dei dati	272
8.16.1 <i>L’interessato</i>	273
8.16.2 <i>Il titolare del trattamento dati</i>	274
8.16.3 <i>Il Data Protection Officer</i>	276
8.16.4 <i>Il responsabile al trattamento</i>	277
8.16.5 <i>L’incaricato al trattamento dei dati</i>	279
CAPITOLO 9 · IL RAPPORTO GIURIDICO DI TRATTAMENTO DEI DATI	281
9.1 Obbligatorio: dal consenso informato al “contratto di trattamento”	283
9.1.1 <i>Le “parti del contratto”</i>	285
9.1.2 <i>Le tre forme di “contratto di trattamento”</i>	286
9.1.3 <i>Il notice-and-consent</i>	287

9.1.4 Il “contratto”	292
9.1.5 Per facta concludentia	293
9.1.6 Il contenuto del contratto di trattamento	294
9.1.7 Gli obblighi assunti dalle parti ed i relativi effetti	296
9.1.8 Ex post: le modifiche al rapporto giuridico	301
9.1.9 Qualche “utile” considerazione a margine	302
9.2 Facoltativo: l’esternalizzazione al responsabile al trattamento	306
9.2.1 L’outsourcing	307
9.2.2 L’outsourcee titolare e l’outsourcer responsabile esterno	310
9.2.3 La responsabilità in eligendo ed in vigilando	313
9.2.4 Il contratto integrato di outsourcing e di nomina a responsabile	315
 CAPITOLO 10 · IL TRATTAMENTO DEI DATI NEL MODELLO EX D.LGS. 231/2001	
EX D.LGS. 231/2001	319
10.1 Il rapporto tra GDPR ed il modello ex D.Lgs. 231/2001	320
10.2 La centralità della persona e la Digital & Security Awareness	324
 BIBLIOGRAFIA	333
 FONTI	349

INTRODUZIONE

Vivere nella dimensione digitale significa essere consapevoli di un presente che rapidamente diventa futuro: nulla di più normale salvo, responsabilmente, comprendere chi guida questo cambiamento.

Questo libro non vuole e non può puntare ad essere esaustivo proprio in relazione alla irrefrenabile dinamica evolutiva del *cyber-space* e della “sfera digitale”: ha l’obiettivo, più umile, di costruire un quadro sinottico dello stato dell’arte, come punto di partenza per un percorso di consapevolezza, che si muove tra aspetti etici, giuridici e tecnici, per consentire e favorire – seppur nella modernità dei cambiamenti – ancora uno sviluppo umano integrale.

Non si tratta solamente di garantire un elevato livello di istruzione (processo top-down), ma di favorire ed avviare la diffusione di una *e-education* che punti a colmare i significativi gap legati alla scarsa cultura sull’utilizzo degli strumenti informatici e sull’etica della *privacy* (sugli aspetti giuridici e sociali della dimensione digitale), sia in termini di percezione verso se stessi, sia verso gli altri.

È necessario avere una visione complessiva a 360° sulle interazioni, sulle relazioni e sugli impatti (tanto sociali, quanto giuridici ed economici) che la nuova dimensione crea ogni giorno sulla società e sui mercati.

Il *fil rouge* è come questi legami si coniugano e vengono regolati e regolamentati: sono, infatti, molteplici le questioni di carattere giuridico-legale che molto spesso vengono sottovalutate.

Tanto a livello individuale, quanto collettivo.

Esiste un macroproblema, ben noto quantomeno alle istituzioni sovranazionali, legato alla sicurezza (collettiva ed individuale, appunto) che si ripercuote – anche – in ambito economico-finanziario.

Infatti «l'azione dell'UE non si limita al solo aspetto *security*, ma tende anche ad intravedere le potenzialità e le opportunità offerte dall'arena digitale anche da un punto di vista economico.

In questo modo, attraverso un approccio di “sicurezza fin dalla produzione” (*security by design*) si tenderà a creare un circolo virtuoso basato sugli investimenti in ricerca e sviluppo per prodotti e servizi “certificati” i quali, in ultima analisi, avranno una ricaduta positiva sull'innalzamento del livello di sicurezza informatica dell'UE.

Il cardine dell'azione operativa svolta dall'Unione Europea nel settore cyber è sempre l'obiettivo strategico che porterà ad un innalzamento della consapevolezza dei cittadini e dei *policy-maker* sulle minacce provenienti dal dominio cyber» (Proli e Valguarnera, 2018).

Per tale ragione, per affrontare in modo proficuo una tematica – normalmente nota per gli esperti di informatica giuridica o di diritto dell'informatica – da una prospettiva diversa sembra opportuno richiamare e partire da un caposaldo riportato all'articolo 3 della Costituzione italiana, seppur in un'ottica più ampia del contesto europeo ed internazionale.

«Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine econo-

mico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese».

La “persona umana” è al centro della nuova dimensione digitale, vivendo spesso le innovazioni tecnologiche con una difficoltà a comprenderne le “regole del gioco”: l'obiettivo è, dunque, “informare” ogni cittadino sui pericoli derivanti e su come la legislazione (vigente ma in continua evoluzione) viene applicata.

D'altronde questo è anche l'orientamento della Commissione europea, promuovendo sempre più campagne di sensibilizzazione sulle cyberminacce, favorendo la divulgazione di una cultura sulla *cyberigiene* non solo tra gli operatori economici ma soprattutto tra i cittadini (ossia i “semplici utenti”), con l'obiettivo di creare un sistema di “deterrenza attiva” (tanto individuale quanto collettiva), ossia di ridurre il numero degli incidenti, delle violazioni e degli attacchi, attraverso l'attenzione, la consapevolezza ed il buon senso.

Con questo libro si vuole percorrere un piccolo sentiero che, partendo dalla “globalizzazione” e dai presupposti essenziali della nascita della “dimensione digitale”, vuole gettare le basi per comprendere quali siano le opportunità e le minacce tanto nei rapporti privatistici quanto nell'*e-government*.

La comprensione di cosa sia il cyberspace e l'evoluzione dei reati, degli illeciti e dei fenomeni criminali (cybercrime) ad esso correlati e conseguenti, passa necessariamente dalla consapevolezza di quali siano le moderne modalità e tecniche informatiche per commetterli: solo attraverso la conoscenza possiamo difendere i nostri diritti e la nostra privacy.

Il sentiero ci conduce, al termine del libro, a comprendere le novità introdotte dal nuovo Regolamento Generale sulla Protezione dei Dati (GDPR): lo spirito del legislatore europeo è una azione positiva di tutela della persona umana, che passa attraverso processi di responsabilizzazione individuale e collettiva. Alcuni spunti operativi, ad esempio, possono aiutare ad individuare le diverse forme di contratto per regolamentare i rapporti giuridici di trattamento dei dati tra i diversi attori produttivi, anche attraverso l'integrazione nel MOGC *ex* D.Lgs. 231/2001.