SOMMARIO

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 *cyberspace* 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 *cyberhygiene* 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.