

N. FABIANO, *GDPR & Privacy. Consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity*, Firenze, goWare, 2019, 178 pp.

Il volume è frutto di un lavoro condotto dal Presidente dell’Autorità per la protezione dei dati personali di San Marino, pubblicato ad un anno dall’entrata in vigore del Regolamento UE 2016/679 (General Data Protection Regulation - GDPR) avente ad oggetto la protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. Alla luce delle novità normative introdotte a livello europeo, il volume è pensato come strumento divulgativo, poiché fornisce uno sguardo d’insieme dell’argomento per poi dettagliarne gli aspetti più significativi. L’Autore intende sottolineare l’importanza della riforma che il GDPR ha apportato in materia di protezione dei dati personali, sottolineando il fatto che esso mira indubbiamente alla protezione dei dati personali, ma nella prospettiva della possibilità della loro circolazione.

Fondamentale risulta essere la distinzione tra *privacy* e *data protection*, diritti fondamentali riconosciuti e garantiti dall’ordinamento giuridico, spesso erroneamente confusi. Per comprendere l’importanza del dato personale è necessario partire dall’assioma che esso è in primo luogo un valore assoluto, proprio come la vita umana. Fabiano afferma infatti: «riteniamo che la vita sia un valore assoluto e inviolabile, perché è la stessa natura che ci permette di affermarlo. Si tratta di un elemento ontologico: la vita è un valore. Allo stesso modo il dato personale si riferisce a informazioni personalissime di una persona fisica e va considerato un valore ontologicamente assoluto».

Si rimarca in più occasioni la necessità che ogni individuo acquisisca consapevolezza del valore dei dati personali, intesa come conoscenza delle modalità con le quali i dati del soggetto vengono trattati. Per essere consapevoli occorre cogliere le opportunità fornite, essere responsabili nell’utilizzo e nella diffusione delle informazioni personali, prestando massima attenzione al soggetto al quale si trasmettono. Si parla in tale ultimo caso di *accountability*, fulcro del nuovo sistema introdotto con il Regolamento europeo e termine del tutto nuovo per l’ordinamento giuridico italiano, che può essere tradotto e interpretato come “responsabilità” o “responsabilizzazione” del titolare del trattamento. In altre parole, è «l’adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento». In tal modo si affida direttamente al titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati nel Regolamento.

Contestualmente si esamina il principio della “protezione dei dati fin dalla progettazione”

(*by design*) e della “protezione per impostazione predefinita” (*by default*). Si tratta della necessità di configurare il trattamento prevedendo fin dall’inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e di tutelare i diritti degli interessati, tenendo conto del contesto globale del trattamento e dei rischi per i diritti e le libertà degli interessati. Tutto ciò deve avvenire *ab initio*, ossia prima di procedere al trattamento dei dati vero e proprio e richiede un’analisi preventiva e un onere applicativo da parte dei titolari.

Il tema su cui si concentra il volume è la *cybersicurity*, che «consiste nelle attività finalizzate alla protezione di un sistema informatico, in modo che esso sia disponibile, autentico ed integro». La sicurezza informatica dovrebbe essere il fondamento della sicurezza nazionale e di tutto ciò che è digitalizzato. È un tema di rilevante importanza che spesso viene ignorato, sicché l’Autore fornisce una sorta di “manuale delle istruzioni” per muoversi in Internet, per l’utilizzo dei *social network* e dei sistemi di messaggistica, affrontando anche il tema delicato della protezione dei minori su Internet.

Inoltre, l’Autore analizza il fenomeno della *blockchain*. Letteralmente si traduce in italiano «come “catena di blocchi”, ma in realtà con l’espressione *blockchain* si fa riferimento ad un sistema informatico attraverso il quale complesse operazioni algoritmiche generano singoli blocchi collegati tra di loro in modo da creare una catena, di qui “catena di blocchi”». La *blockchain* è pertanto «un database con caratteristiche particolari, in cui ciascun record è costituito da un nodo (che a sua volta contiene informazioni) e i singoli nodi sono legati l’uno all’altro in modo da non poter essere modificati e quindi da non poter compromettere l’intera catena». Tale strumento ha consentito lo sviluppo del *Bitcoin* e delle altre criptovalute, che consentono l’abbattimento dei costi, l’eliminazione di intermediari, la semplificazione delle operazioni e la sicurezza delle transazioni.

Infine, l’Autore mette in luce i profili etici dell’intelligenza artificiale e della protezione dei dati personali attraverso il ricorso ai principi di «liceità, correttezza e trasparenza», «limitazione della finalità», «limitazione della conservazione», «integrità e riservatezza», tutti sanciti dall’art. 5, par. 1, lett. a), del GDPR. L’Autore invita pertanto a guardare il mondo digitale con consapevolezza e responsabilità, affinché «si lavori per consolidare e accrescere una vera consapevolezza del valore della persona e dell’intera sfera di ciascun individuo in modo che non venga mai svilita la dignità umana».

SILVIA BIANCHI