LA PRIVACY 2.0 È TUTTA EUROPEA

di UMBERTO RAPETTO
Generale (R) della Guardia di Finanza – cyber security advisor

È la sigla che maggiormente ha saputo rimbombare negli ultimi mesi. "Gdpr" ha martellato la mente anche dei più distratti, generando una sorta di contaminazione che ha portato a mescolarne la sequenza delle lettere, quasi che l'errore di dizione fosse il primo sintomo di un indomabile spavento.
Chiunque l'abbia pronunciata recentemente lo ha fatto per saperne qualcosa di più su una questione imprescindibile come la riservatezza dei dati personali. L'interesse non è certo quello della tutela dei fondamentali diritti civili, ma viene piuttosto dettato dalla necessità di mettersi in regola per evitare sanzioni che possono arrivare a 20 milioni di euro o a un terrificante 4% del fatturato globale.
Stiamo parlando, è fin troppo ovvio, della maturata operatività il 25 maggio scorso del Regolamento europeo 679 in tema di privacy, provvedimento che è impossibile considerare una novità, visto che era stato pubblicato sulla Gazzetta Ufficiale Ue due anni prima. Il tempo concesso per adeguarsi alla nuova normativa lascia intendere che la disciplina in materia di protezione delle informazioni personali è giunta a un punto di arrivo. Al contempo offre l'opportunità per capire che – come tanti altri indigesti provvedimenti comunitari – la legge sarà inesorabilmente uguale per tutti. Poco, forse nullo, lo spazio a disposizione degli Stati membri per personalizzare l'applicazione e, inevitabile conseguenza, pressoché assente la possibilità di "sconti" nazionali per particolari categorie o specifici adempimenti.

Norme in evoluzione nel tempo

Il Regolamento 679 è l'ultima tappa di un lungo percorso cominciato con la Direttiva 46 del 1995 emanata con l'obiettivo, tanto ambizioso quanto tradito, di armonizzare in ambito europeo le normative vigenti o promulgande nei diversi territori continentali.
Il recepimento di tale direttiva in Italia si è tradotto nella legge 675 del 1996 che per la prima volta ha inserito nel nostro ordinamento norme basilari per la tutela delle persone rispetto il trattamento delle informazioni a loro riferite. L'impatto (e non c'è bisogno di memoria straordinaria per ricordarlo) fu abbastanza traumatico sia in termini organizzativi, sia nei suoi riflessi finanziari per oneri e spese fino a quel momento imprevedibili. Saltò fuori l'informativa da rilasciare ai soggetti interessati, si materializzò l'obbligo di acquisire il consenso al trattamento dei dati, vennero fuori vincoli su quelli considerati "sensibili" (razza, etnia,

opinioni politiche, convinzioni religiose o filosofiche, iscrizioni sindacali o ad associazioni, vita sessuale e condizioni di salute), cambiò sostanzialmente la gestione degli archivi e il rapporto con i soggetti le cui informazioni erano il motore di mille attività.
L'Autorità Garante – all'epoca neo costituita – si trovò a gestire una situazione tutt'altro che agevole, costretta a predisporre provvedimenti di ogni natura (facendo addirittura ricorso a comunicati stampa certo inusuali in ambito regolatorio) per fronteggiare lo tsunami di richieste e sollecitazioni provenienti da enti pubblici, associazioni di categoria, aziende e realtà più disparate.
Nel 2003 c'è stata la prima grande svolta con il varo del decreto legislativo 30 giugno 2003 n° 196, noto ai più come il "Codice della Privacy", opportunamente corredato di una serie di "Allegati" di cui il "B" ha assunto il ruolo di vera e propria bussola per le misure di sicurezza da adottare a protezione dei dati.

Il peso delle responsabilità

Purtroppo l'eutrofia normativa ha determinato uno sviluppo incontrollato della disciplina, e ciascun Paese ha intrapreso strade autonome e non sempre allineate ai principi originari, costringendo Bruxelles a riprendere il timone di un bastimento altrimenti destinato alla deriva.
Il Regolamento europeo ribadisce molti dei cardini su cui era imperniata la precedente normativa, ma va a introdurre una serie di novità che non si limitano alle lievitate roboanti sanzioni in grado di spaventare persino i più spregiudicati utilizzatori indebiti di dati personali.
La pietra d'angolo è rappresentata dai concetti di "privacy by design" e "privacy by default", ovvero della protezione dei dati originata in sede di progettazione degli strumenti tecnologici e delle procedure con cui si eseguono i trattamenti dei dati e della protezione predefinita. Il cosiddetto "titolare del trattamento" – privato delle indicazioni puntuali che in Italia provenivano dall'Allegato B – deve tenere conto di una serie di fattori fondamentali (stato dell'arte, costi attuativi, natura e ambito di contesto e finalità del trattamento, rischi e relativa pericolosità per i diritti) e porre in essere misure tecniche e organizzative adeguate (assumendosene la relativa responsabilità) per offrire le massime garanzie a tutela dei diritti degli interessati e a dimostrazione della conformità dei trattamenti ai requisiti stabiliti dal Regolamento 679.
La responsabilizzazione ("accountability", come la indicano gli appassionati anglofoni) è innescata dal dovere in capo al titolare di assicurare costantemente il rispetto dei principi sanciti e l'immediata comunicazione (da un lato all'Autorità di Controllo o Garante, dall'altro ai soggetti cui si riferiscono i dati) dell'eventuale violazione di informazioni personali. Le 72 ore di tempo dalla scoperta del misfatto costituiranno la scadenza di una serie di attività conseguenti la rilevazione dell'accaduto: il termine "data breach" (equivalente alla breccia illecitamente aperta nelle virtuali mura perimetrali dei grandi archivi elettronici) è destinato a rientrare nelle priorità operative di chi tratta enormi masse di informazioni e le iniziative da avviare per ristabilire la normalità e per rimediare (eliminando o riducendo le conseguenze negative) dovranno essere previste e pianificate nel minimo dettaglio.
Sul palcoscenico della privacy in versione europea appare poi un nuovo personaggio etichettato come "Data protection officer" o "Dpo", ovvero il responsabile della protezione dei dati personali, previsto per sottolineare il ruolo della sicurezza e ribadita la necessità che venga costituita una figura di supporto con un ruolo di costruttivo contraddittorio con il titolare. Il Dpo (o "Rpd" per trovare un acronimo nostrano) avrà compiti di consulenza e supervisione e sarà la qualificata interfaccia tra titolare e Autorità Garante, una sorta di segnale che la "privacy 2.0" sarà qualcosa di più "serio" e concreto di quanto non abbia invece caratterizzato il passato.