Privacy

Il principio di accountability: la silente rivoluzione nella protezione dei dati

di **Vincenzo Colarocco**

Uno dei pilastri fondamentali del Regolamento Europeo 679/16 per la protezione dei dati personali (GDPR) è il principio di *accountability* che sta rivoluzionando l'approccio nei riguardi della *data protection*.

Il *Working Party* 29 (WP29) con il parere 3/2010 ha rappresentato, già nel luglio del 2010, come i principi e gli obblighi dell'Unione europea in materia di protezione dei dati siano spesso applicati in modo insufficiente cagionando di fatto una lesione dei diritti degli interessati. Ed infatti se la protezione dei dati non fosse diventata **parte integrante** delle pratiche e dei **valori condivisi** di un'organizzazione e se le relative responsabilità non fossero state espressamente ripartite, il rispetto effettivo delle norme in materia di protezione dei dati sarebbe stato messo notevolmente a rischio e gli incidenti in questo settore sarebbero inevitabilmente continuati.

Proprio per questa ragione, il WP29 ha avanzato una proposta concreta per l'introduzione di un principio di responsabilità che richiede ai titolari del trattamento di mettere in atto misure adeguate ed efficaci per garantire il rispetto dei principi e degli obblighi stabiliti nella direttiva. La *ratio* è quella di passare "dalla teoria alla pratica", garantire la certezza del diritto, pur ammettendo, al tempo stesso, una certa flessibilità, sì da consentire la determinazione delle misure concrete da applicare in funzione dei rischi connessi al trattamento dei dati, avuto riguardo delle differenti tipologie degli stessi.

Dunque, sul solco tracciato dal WP29 il GDPR con il Considerando 74 ha, sin da subito, precisato l'opportunità di stabilire la **responsabilità generale del titolare** del trattamento per qualsiasi utilizzazione di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci **dimostrando la conformità** delle attività di trattamento con il Regolamento. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

A ciò si aggiunga che il **principio di *accountability* è trasversale** all'intero impianto normativo del GDPR, basti pensare all'articolo 5 par. 2 ove "*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione)*" ed all'articolo 24 par. 1 "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del*

trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

Dunque, il Regolamento **rovescia la prospettiva** della disciplina in materia di protezione dei dati personali in quanto **tutto** il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del **titolare** del trattamento, il quale determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza ed ha **maggiore discrezionalità** nel decidere come conformarsi alle disposizioni del GDPR, pur avendo **l'onere di motivare** le ragioni a supporto di tali decisioni dimostrandone la conformità al Regolamento.

Ulteriore forza propulsiva del principio dell'***accountability*** è data dall'applicabilità dello stesso **a tutti i soggetti** che trattano dati personali e non solo al titolare del trattamento, ma anche al responsabile (artt. 28.1 ("*garanzie sufficienti*"), al *Data Protection Officer* (art. 37.5 "*conoscenza specialistica della materia e delle prassi*"), alle persone autorizzate o designate (art. 39.1.b "*formazione e sensibilizzazione del personale*"). Ed è proprio in questa ottica che si riesce a passare "dalla teoria alla pratica", garantendo la **concreta applicabilità** della protezione dei dati personali, riducendo sostanzialmente i rischi connessi al trattamento e alla tipologia di dati trattati. Del resto il principio di *accountability* ben potrebbe tradursi anche nel principio di **consapevolezza** secondo il quale ogni individuo conosce i rischi ed i diritti propri della società dell'informazione o meglio della società *data driven*.

Proprio in tale ottica il principio di *accountability* permea tutta la struttura del GDPR, sì da coinvolgere anche la **revisione dei processi**, ed infatti il titolare deve riesaminare ed aggiornare le misure adottate rivalutando anche la valutazione di impatto almeno quando insorgono variazioni del rischio e, insieme al responsabile, assicurare su base continua riservatezza, integrità, disponibilità, resilienza dei sistemi tecnologici.

A ciò si aggiunga che la protezione dei dati personali, intrinsecamente dinamica, stante la stretta correlazione con le nuove tecnologie, ha la sua chiave di volta nel **rischio** per i diritti e le libertà dell'interessato, da intendersi a mero titolo esemplificativo come: perdita del controllo dei dati personali; limitazione di diritti; discriminazione; furto o usurpazione d'identità; perdite finanziarie; decifratura non autorizzata pseudonimizzazione; pregiudizio alla reputazione; compromissione del segreto professionale; qualsiasi altro danno economico o sociale significativo alla persona fisica, ecc.

Dunque, il principio di *accountability* può esser soddisfatto attraverso gli strumenti necessari idonei a mettere in pratica misure efficaci come le procedure per garantire l'identificazione di tutte le operazioni di trattamento dei dati e per rispondere alle richieste di accesso, lo stanziamento di risorse e la designazione di persone responsabili per l'organizzazione della conformità della protezione dei dati, la gestione dinamica del registro dei trattamenti.

In **conclusione**, lo sviluppo di nuove tecnologie e la costante globalizzazione dell'economia e

della società hanno condotto ad una proliferazione di dati personali raccolti, selezionati, trasferiti o altrimenti conservati. I rischi connessi a tali dati, pertanto, si sono moltiplicati.

L'aumento sia dei rischi sia del valore dei dati personali in sé determina la necessità di rafforzare il ruolo che il titolare del trattamento – adottando un **approccio proattivo** e **dinamico –** è chiamato ad individuare e ad applicare mediante **misure** appropriate, **concrete** ed **efficaci**, al fine di realizzare i risultati richiesti dal GDPR.

Tutto ciò attraverso la creazione di **cultura** e consapevolezza all'interno della propria realtà.