EDITORIALE: La protezione del dato personale non è solo questione di sicurezza informatica, anzi…

Andrea Lisi - *Direttore Editoriale KnowIT, Studio Legale Lisi - www.studiolegalelisi.it*

Ultimamente si ascolta troppo spesso l'affermazione, riferita dai tanti nuovi "esperti della materia" (spuntati in giro come funghi), che l'adeguamento al GDPR (*General Data Protection Regulation* – Regolamento 679/2016) sarebbe al 90% questione di sicurezza informatica. In assenza di specifiche argomentazioni a sostegno di questa tesi, solitamente i discorsi proseguono con un elenco di improbabili ricette miracolose, tutte strettamente informatiche (e poco decifrabili da chi non è alfabetizzato in materia), che consentirebbero a qualsiasi organizzazione (pubblica o privata che sia) di superare indenne la fatidica data del 25 maggio 2018. Data in cui, come ben sappiamo, il GDPR diventerà pienamente esecutivo.

Non c'è nulla di più assurdo e sbagliato di queste prese di posizione. Sviluppare a casaccio straordinarie procedure di sicurezza informatica, elencando scienza crittografica, tecniche di pseudonimizzazione, azioni di *penetration test*, analisi dei rischi, *Privacy Impact Assessment*, *gap analysis* e così via, in un fritto misto incomprensibile e indigesto, non serve a nulla.

Le politiche di sicurezza informatica vanno infatti precedute da un'organizzata verifica e da un'approfondita mappatura di strumenti, persone, sistemi, banche dati, applicativi e procedure che servono all'impresa o alla PA per sviluppare trattamenti di dati. Dopo questa forma di "registrazione affidabile" di tutto ciò che ha a che fare con il trattamento dei dati personali, occorrerà procedere con una verifica dettagliata dei flussi (interni ed esterni) in cui sono coinvolti tali dati e quindi delle aree più critiche e sensibili, per poi proseguire sviluppando una corretta organizzazione a tutela dei dati mappati. E quell'organizzazione è fatta, prima di tutto, di risorse umane che vanno istruite, di processi e procedure che vanno posti in essere a presidio del corretto trattamento e a protezione dei vari perimetri individuati e degli specifici rischi insiti in ognuno di quei perimetri. Solo dopo questa approfondita e documentata azione di carattere giuridico/organizzativo/manageriale sarà possibile procedere con un *Privacy Impact Assessment* per le aree a maggior rischio individuate e predisporre così adeguate misure di sicurezza, anche di carattere informatico.

Questa è, quindi, l'*accountability* di cui tanto si parla e discute in questi giorni e che prevede, così, che il Titolare del trattamento debba essere in grado di dimostrare di aver adottato un processo complessivo di misure giuridiche, organizzative, tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi (in qualche modo analoghi a quelli utilizzati nell'applicazione del D.lgs. 231/2001).

Aziende e PA devono pertanto dotarsi di strumenti per valutare lo stato della propria *accountability* (secondo i principi della *privacy by design* e *privacy by default*) e dimostrarlo all'Autorità Garante. Infatti, il Regolamento UE 2016/679 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.

Questa impostazione, che in qualche modo comporta per i Titolari (e i Responsabili del trattamento) il dovere costante di dimostrare di avere effettuato un'approfondita autoanalisi seguita da opportune scelte ben ponderate e documentate, si ritrova anche nell'apparato sanzionatorio, dove la gravità delle sanzioni segue i principi dell'*accountability*, rendendo più gravi proprio quei comportamenti che si discostino da tali principi e/o dal generale dovere di trasparenza, di organizzazione e di adeguata documentazione delle scelte effettuate.

Infatti, le inadempienze più gravi previste dal GDPR (che comportano l'applicazione di sanzioni amministrative pecuniarie fino a 20.000.000 di euro o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) sono riconducibili alla violazione delle seguenti fattispecie:

a) principi generali applicabili al trattamento (art. 5), condizioni di liceità del trattamento (art. 6), condizioni per il consenso (art. 7) e trattamento di categorie particolari di dati personali (art. 9);

b) diritti degli interessati (artt. da 12 a 22);

c) trasferimenti di dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale (artt. da 44 a 49);

d) obblighi previsti dalle legislazioni degli Stati membri adottate a norma del capo IX (giornalismo, espressione accademica o letteraria, accesso ai documenti delle PA, rapporti di lavoro, archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica);

e) negato accesso all'autorità di controllo durante l'esercizio dei propri poteri di indagine o inosservanza di un suo provvedimento di carattere correttivo.

Mentre le sanzioni più lievi (pur se sempre di grande rilievo economico, perché comportano l'applicazione di sanzioni amministrative pecuniarie fino a 10.000.000 di euro o, per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) sono riconducibili a violazioni per lo più legate a procedure di sicurezza informatica o a procedure specifiche quali:

a) obblighi del Titolare del trattamento e del Responsabile del trattamento:

- consenso dei minori (art. 8)
- trattamento che non richiede l'identificazione (art. 11)
- principi di *privacy by design* e *by default* (art. 25)
- accordo interno per determinare le responsabilità tra contitolari (art. 26)
- nomina del rappresentante dei Titolari o dei Responsabili non stabiliti nell'Unione e suoi compiti (art. 27)
- compiti e responsabilità del Responsabile del trattamento (art. 28)
- trattamento da parte dei dipendenti e collaboratori del Titolare o del Responsabile (art. 29)
- tenuta dei registri delle attività di trattamento (art. 30)
- cooperazione del Titolare o del Responsabile del trattamento con l'autorità di controllo (art. 31)
- adozione di misure di sicurezza adeguate (art. 32)
- notifica all'autorità di controllo di una violazione di dati personali (art.33)
- comunicazione all'interessato di una violazione di dati personali (art. 34)
- valutazione d'impatto (art. 35)
- consultazione preventiva (art. 36)
- designazione del DPO (art. 37)
- obblighi del Titolare e del Responsabile nei confronti del DPO (art. 38)
- esecuzione dei propri compiti da parte del DPO (art. 39)
- obblighi in materia di certificazione (art. 42);

b) obblighi dell'organismo di certificazione (artt. 42 e 43);

c) obblighi dell'organismo di controllo (art. 41, paragrafo 4).

Occorre pertanto prestare particolare attenzione a non confondere e sovrapporre i due aspetti della protezione e della sicurezza del dato: **l'adeguamento al GDPR – lo ribadiamo – impone non solo l'adozione di nuove misure tecnologiche, ma anche e soprattutto un nuovo approccio legale e organizzativo basato sull'analisi del rischio (e relativa documentazione delle scelte effettuate sulla base della stessa)**. Il rinnovamento dello scenario normativo, infatti, ruota attorno al perno dell'approccio basato sull'**accountability** (ovvero "responsabilizzazione"), che comporta per il Titolare del trattamento l'attuazione di tutte le misure di sicurezza in termini sì tecnologici, ma soprattutto organizzativi, per **dimostrare (documentando appunto)** di aver strutturato i trattamenti di dati personali conformemente ai principi della *privacy by design* e della *privacy by default*.

Per concludere, il Titolare - quale soggetto che determina le finalità e i mezzi del trattamento, nonché le misure (anche tecnologiche) di sicurezza - ha maggiore discrezionalità nel decidere come conformarsi alle disposizioni del nuovo Regolamento, ma ha l'onere di dimostrare le ragioni a supporto di tali decisioni e le motivazioni per cui ritiene che le medesime siano in linea con il Regolamento. **La sicurezza, pertanto, diventa parte integrante della protezione del dato, ma solo in conseguenza di queste scelte documentate**.