Interesse nazionale e sovranità digitale, come tutelare i dati degli enti di ricerca

*Pubblichiamo il testo dell'intervento tenuto da **Lucio Badiali**, DPO, **Istituto Nazionale di Geofisica e Vulcanologia**, al convegno "I Dati tra Sovranità Digitale e Interesse Nazionale. Le Persone, le Pubbliche Amministrazioni e le Imprese", svoltosi nell'Ateneo milanese il 25 novembre scorso.*

In tema di interesse nazionale e sovranità, la Ricerca rappresenta decisamente un *asset* strategico del sistema Paese. La ricerca nazionale è strutturata in circa una ventina di enti. Si va da quelli impegnati in studi sull'agricoltura, a quelli sulle particelle subatomiche, dagli studi sull'universo e alle tecnologie spaziali a quelli che si occupano di ricerca medica, biomedica, dalla genetica alla statistica, c'è chi fa scienze della terra, chi si occupa di ambiente, matematica, lavoro, energie, politiche pubbliche, istruzione e così via.

Come il gatto di Schrödinger, bisognava attendere l'entrata in vigore del GDPR per scoprire gli enti di ricerca non pronti

Ma gli enti di ricerca sono anche una declinazione dell'amministrazione pubblica. E da quel lontano 27 aprile 2016 gli enti, come la gran parte della PA, hanno vissuto in uno stato di indeterminatezza quasi quantistica. Come il gatto di Schrödinger, bisognava attendere il 24 maggio 2018 per scoprire che si sono presentati alla data dell'entrata in

vigore del **GDPR** non così pronti come avrebbero potuto.

Non lo erano i titolari, i quali credevano stesse per sorgeva all'orizzonte solo un ulteriore gravoso adempimento normativo. Cercavano ancora al di fuori le regole cui conformarsi e gli elenchi dettagliati di prescrizioni per i trattamenti. Era troppo fuori dall'esperienza il seguire un modello di responsabilità e rendicontazione dell'operato. L'*accountability*, vera chiave di volta e rivoluzione copernicana nel nuovo mondo della protezione dati e della privacy, come principio sembrava un concetto più teorico che operativo.

Subito dopo il primo passo obbligato, ed eseguito con un po' di inerzia, della nomina dei DPO, i DPO stessi del comparto della ricerca hanno iniziato a cercarsi per scambiare opinioni e valutare le migliori prassi. I Direttori generali, riuniti nella *Conferenza permanente dei Direttori Generali degli Enti Pubblici di Ricerca Italiani* (CO.DI.G.E.R.) intuendo l'importanza del fenomeno emergente, creavano per i DPO il "Tavolo Tecnico sulla Privacy", luogo di incontro dove costruire uno standard operativo per la *data protection* della comunità degli enti ricerca, così da affrontare la sida del nuovo Regolamento. L'obiettivo era quello di fare rete.

Anche il Garante ha guardato a questa attitudine emergente, e l'ha sostenuta facilitandone il compito affidando al tavolo di lavoro un suo dirigente che periodicamente continua ad incontrare i DPO. Un supporto per vedere come cresce la consapevolezza della protezione dati in questa fetta di amministrazione pubblica in un rapporto dialettico fatto di dubbi, domande e risposte.

Oggi i DPO del comparto si sentono più preparati ad affrontare le sfide

Oggi, dopo il primo periodo di rodaggio, i DPO del comparto si sentono più preparati ad affrontare le sfide. Dopo poco più di un anno anche il DPO comincia ad assumere una sembianza più precisa. La sua figura di verifica e garanzia tuttavia non può essere completamente definita in una realtà che è sua volta liquida ed in divenire. Le sue stesse competenze sono messe continuamente in discussione. Come pure quelle degli organi decisionali di un tipico ente di ricerca. Durante i nostri scambi ci domandiamo cosa ci si aspetti da un DPO e in cosa potrebbe evolvere, rispetto a ciò che si è tentato di stabilire finora sia nelle normative nazionali sia in quella europea con un corpus della materia e di competenze che non è più ormai solamente riferibile al GDPR. È il nostro un profilo aziendale molto più sensibile di quello che si è tratteggiato in letteratura e che si è immaginato. Non può limitarsi ad essere presente in un *board*, interagire con il management solo per prevenire contenziosi futuri o interpretare la legge per limitare i danni in una causa per violazione dati. Non possono sfuggirgli le dinamiche e i significati della rivoluzione del big data e le implicazioni per la società come la *privacy by design*, norma cui relazionarsi durante le fasi di organizzazione aziendale.

Una consapevolezza che i DPO hanno raggiunto è che gli stessi organi sociali dovrebbero accrescere le loro conoscenze in ambito di protezione del dato e gestione della sicurezza così da essere consapevoli delle scelte che l'ente compie e poter interagire più naturalmente ed efficacemente con il DPO.

Parafrasando Eraclito di Efeso si potrebbe dire che il compito più difficile di un Protection Officer sarà "aspettarsi l'inaspettato" per non trovarsi impreparato nel momento di

crisi così da poter permettere al titolare di realizzare compiutamente il principio della *accountability*.

Il rispetto della privacy e, più in generale, la difesa del dato personale – specialmente in un ambito di interesse nazionale – presuppone un'adeguata sicurezza. La sola sicurezza, purtroppo, non presuppone il rispetto della privacy e quindi il lavoro ed il ruolo che si sta ritagliando il DPO richiederà una formazione sempre più di studio interdisciplinare per poter interagire e comunicare al meglio ad ogni livello.

https://www.key4biz.it/interesse-nazionale-e-sovranita-digitale-come-tutelare-i-dati-degli-enti-di-ricerca/281026/