BANCA D'ITALIA
EUROSISTEMA

La protezione dei dati personali oggi
Ruoli e responsabilità, nuove competenze, rischi e opportunità

Intervento di Gian Luca Trequattrini
Vice Direttore generale della Banca d'Italia

Network dei Responsabili della Protezione dei Dati
delle autorità amministrative indipendenti

Roma, 26 novembre 2026

La tutela della privacy è al centro di una trasformazione profonda, indotta dalla discontinuità tecnologica che caratterizza il nostro tempo. I Responsabili della Protezione dei Dati sono figure di cerniera in questa trasformazione, il cui mandato non si esaurisce più nel controllo della conformità al GDPR: il compito è ora quello di presidiare un confine sempre più mobile, quello tra la raccolta e il trattamento dei dati e la loro protezione da accessi non autorizzati, usi impropri, tentativi di frode.

Questo confine è diventato difficile da tenere. Le minacce cyber alle infrastrutture pubbliche hanno assunto una dimensione strutturale: non si tratta più di episodi isolati, ma di una pressione continua, esercitata da attori che dispongono di risorse crescenti e di capacità tecniche avanzate. Gli attacchi *ransomware*, le campagne di *phishing* mirate ai dipendenti, le intrusioni nei sistemi di gestione dei dati non sono incidenti di percorso della digitalizzazione, ma sono il riflesso di una vulnerabilità strutturale che richiede risposte altrettanto strutturali.

Le amministrazioni pubbliche dipendono oggi da infrastrutture digitali complesse: servizi cloud, piattaforme di intelligenza artificiale, reti di telecomunicazione, sistemi di interoperabilità tra banche dati. Molte di queste infrastrutture sono gestite da soggetti privati, spesso non europei. Le vulnerabilità non si manifestano soltanto all'interno dei singoli enti: si propagano lungo l'intera catena tecnologica, amplificandosi nei punti di interconnessione tra sistemi diversi. Un fornitore compromesso può diventare vettore di attacco per altre amministrazioni che ne dipendono; una vulnerabilità in un componente condiviso si trasforma in esposizione collettiva.

Il quadro regolamentare europeo ha risposto a questa complessità con strumenti importanti. Il GDPR ha introdotto un approccio fondato sul rischio, che obbliga le organizzazioni a valutare non solo la conformità formale, ma la sostanza della protezione e impone, in caso di violazione, obblighi di notifica che presuppongono sistemi di rilevamento adeguati. L'*AI Act* ha esteso questa logica ai sistemi di

intelligenza artificiale, classificando il rischio in funzione dell'impatto sui diritti fondamentali. Il D*igital Operational Resilience Act* (Regolamento DORA), pensato per il settore finanziario ma indicativo di una tendenza più ampia, ha introdotto un principio che riguarda tutte le istituzioni: la resilienza operativa non è una questione che si risolve all'interno del singolo ente, ma dipende dalla tenuta dell'intero ecosistema tecnologico.

DORA affronta esplicitamente il rischio di concentrazione: la dipendenza da un numero ristretto di fornitori tecnologici critici non è solo un problema di continuità operativa, è un problema di autonomia strategica, di sovranità digitale. Quando un'infrastruttura condivisa viene meno – per una scelta commerciale, per un incidente, per una pressione geopolitica – le conseguenze si propagano istantaneamente a tutti i soggetti che vi si appoggiano.

Su questo punto vale richiamare un principio che DORA ha reso operativo nel settore finanziario e che dovrebbe ispirare anche la Pubblica Amministrazione: la condivisione delle informazioni sulle minacce, il cosiddetto *threat intelligence sharing*. La cybersicurezza non può essere affrontata come una sfida individuale. Ogni ente che affronta un attacco o rileva una vulnerabilità dispone di informazioni che, se condivise tempestivamente con gli altri, diventano difese preventive. La frammentazione di queste informazioni riduce la resilienza collettiva; la loro circolazione in canali protetti la rafforza. Un sistema in cui ciascuna amministrazione gestisce gli incidenti in solitudine è strutturalmente inferiore a uno in cui le esperienze diventano patrimonio condiviso.

Vi è poi un nesso specifico tra privacy e cybersicurezza che merita attenzione. I due ambiti sono spesso trattati come domini separati, perché nell'opinione comune la protezione dei dati è colta come una questione giuridica e la sicurezza informatica come una questione tecnica: ebbene, questa separazione è sempre meno sostenibile. Una violazione di sicurezza è, nella quasi totalità dei casi, anche una violazione dei dati personali: i sistemi che non sono sicuri non sono sistemi che tutelano i diritti. Viceversa, una gestione dei dati che non rispetta i principi di minimizzazione e limitazione della conservazione amplia inutilmente la superficie di attacco: dati che non dovrebbero essere conservati, se lo sono, diventano un rischio in più. Privacy e sicurezza si rafforzano reciprocamente quando sono progettate insieme e si indeboliscono reciprocamente quando vengono governate in silos separati.

Da qualche tempo si parla delle prospettive legate alla diffusione in molti ambiti di infrastrutture basate su tecnologie a registro distribuito, tra cui le *blockchain*. Si tratta di architetture che presentano proprietà di sicurezza notevoli: la struttura a catena di blocchi crittograficamente collegati rende estremamente difficile alterare retroattivamente i dati registrati e la natura distribuita del registro elimina i punti singoli di guasto tipici delle architetture centralizzate. Per alcune funzioni pubbliche, quali la certificazione di atti, la tracciabilità di procedure amministrative, la gestione di identità digitali, queste proprietà sono genuinamente attraenti.

Tuttavia, la stessa caratteristica che rende la *blockchain* sicura sotto il profilo dell'integrità dei dati la rende problematica sotto il profilo della protezione di quelli personali. L'immutabilità del registro, cioè il fatto che ciò che viene scritto non può essere cancellato, entra in collisione frontale con alcuni dei diritti fondamentali sanciti dal GDPR: il diritto alla rettifica dei dati inesatti, alla cancellazione, all'oblio. Se un dato personale viene registrato su una *blockchain* pubblica o anche su una *blockchain permissioned* con nodi diffusi, esercitare questi diritti diventa tecnicamente arduo, talvolta impossibile. Il Comitato Europeo per la Protezione dei Dati e diverse autorità nazionali di controllo hanno già affrontato questa tensione, indicando che la compatibilità con il GDPR dipende in modo critico dalle scelte architetturali: quali dati vengono effettivamente scritti sul registro, in quale forma, con quale livello di accessibilità.

La risposta non è necessariamente la rinuncia a queste tecnologie, ma piuttosto la consapevolezza delle loro implicazioni. Alcune soluzioni tecniche consentono di attenuare la tensione: scrivere sul registro distribuito soltanto *hash* crittografici dei documenti, impronte digitali che ne certificano l'autenticità senza contenere dati personali in chiaro, conservando i dati effettivi in archivi separati e modificabili; oppure ricorrere a tecniche crittografiche avanzate che permettono di verificare la correttezza di un'informazione senza rivelarne il contenuto. Queste soluzioni richiedono competenze specialistiche elevate che non sono patrimonio diffuso nelle amministrazioni pubbliche, che continuano a soffrire la difficoltà strutturale di attrarre e trattenere professionalità tecniche e digitali per le quali la competizione con il settore privato è particolarmente intensa; richiedono inoltre una progettazione accurata fin dalle prime fasi: non sono correzioni che si possono applicare a posteriori su sistemi già in produzione.

Credo che ne possiamo trarre una conclusione di carattere generale, che vale oggi più che mai: per i Responsabili della Protezione dei Dati il momento dell'intervento è la fase della progettazione, non quella della verifica finale. La Valutazione d'Impatto sulla Protezione dei Dati – la cosiddetta DPIA – deve essere condotta prima che le scelte architetturali siano consolidate, quando è ancora possibile orientarle. Un'amministrazione che si presenta al RPD con un sistema già sviluppato, chiedendo una validazione ex post, ha già ristretto lo spazio di manovra in modo significativo. La *privacy by design* non è una formula retorica, ma una condizione operativa che presuppone il coinvolgimento del RPD nelle fasi iniziali di ogni progetto che tratti dati personali, indipendentemente dalla tecnologia impiegata.

Il ruolo dei Responsabili della Protezione dei Dati è, in questo contesto, davvero strategico. Non si tratta soltanto di verificare che i trattamenti siano conformi, ma di portare all'interno delle organizzazioni una visione integrata del rischio che tenga insieme la dimensione giuridica e quella tecnica. Questo richiede interlocuzione continuativa con i responsabili dei sistemi informativi, con i fornitori, con le strutture di audit interno e, sempre più, con le omologhe figure di altri enti, in un'ottica di collaborazione che superi i confini della singola amministrazione.

Questa riunione è l'occasione per fare il punto su come viene affrontata questa doppia sfida: quali strumenti di governo del rischio sono stati adottati, dove persistono lacune, come rafforzare la collaborazione per sviluppare competenze condivise e ridurre le asimmetrie di capacità tra enti grandi e piccoli. I Responsabili della Protezione dei Dati sono una rete naturale per questo scambio: condividete lo stesso mandato, affrontate gli stessi problemi e potete costruire insieme risposte più robuste di quelle che ciascuno può elaborare isolatamente.

Lascio ora spazio al lavoro comune, con l'auspicio che da questa giornata emergano indicazioni concrete su cui costruire i passi successivi.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia