BANCA D'ITALIA
EUROSISTEMA

Protezione dei dati personali – Assetti organizzativi e problemi operativi del RPD in Banca d'Italia

Intervento di Gian Luca Trequattrini
Responsabile della protezione dei dati della Banca d'Italia

Webinar Istat "La protezione dei dati personali", 23 giugno 2021

Autorevoli colleghi, partecipanti al seminario,

il Responsabile della protezione dei dati (RPD) in Banca d'Italia prende forma nel 2018 e consegue all'applicazione del Regolamento generale europeo di due anni prima. Altri ordinamenti hanno preceduto, sin da epoche ormai remote, la soluzione condivisa nell'Unione Europea, se è vero che la prima comparsa di questa figura risale al 1970 in Germania e al 1999 negli USA.

I molteplici ruoli che gli sono assegnati dalla normativa - consulenza nei confronti del titolare del trattamento, sorveglianza sul rispetto delle norme in materia di *privacy*, cooperazione e raccordo con il Garante per la protezione dei dati personali - unitamente ai requisiti di autonomia richiesti dal Regolamento UE

hanno indotto la Banca a porre il RPD in una posizione organizzativa che assicurasse di "*poter adempiere alle funzioni e ai compiti … incombenti in maniera indipendente*" (riprendo il Considerando 97 del Regolamento). L'incarico è stato assegnato al Revisore Generale, uno dei dodici Funzionari Generali, preposto alla funzione di *internal audit* e in posizione di indipendenza rispetto alle funzioni di *business* istituzionali e aziendali.

Tale collocazione, decisa dopo un ampio dibattito interno, fu ritenuta la migliore possibile – nell'assetto della Banca – per prevenire conflitti di interessi, evitando che il RPD si trovasse a esercitare un ruolo che comportasse la definizione delle finalità o delle modalità di un trattamento di dati personali. Questa soluzione consente, fra l'altro, un adeguato contraddittorio con il titolare del trattamento, compito che nell'Istituto è stato delegato dal Direttore Generale al Servizio Organizzazione, una struttura di coordinamento del sistema di pianificazione e controllo strategico che si occupa di sviluppo dell'organizzazione e delle *policy* aziendali di gestione del rischio operativo.

Per lo svolgimento delle attività di analisi istruttoria, in via transitoria e in attesa che l'operatività si consolidasse, si decise di non procedere alla costituzione di una struttura di supporto ma, in relazione all'attribuzione del ruolo di RPD a una posizione di elevato livello collocata fuori dai Dipartimenti, di prevedere solo singole risorse in staff. È stata però di recente approvata dal Direttorio della Banca la costituzione di un nucleo di segreteria tecnica, posto alle dirette dipendenze del RPD e non inquadrato in altre strutture organizzative, con una dotazione iniziale di organico di 4/5 addetti.

Si tratta di una soluzione non isolata nell'ambito dell'Eurosistema. Prima di proporre al Direttorio la costituzione del

Nucleo di segreteria abbiamo infatti interpellato la Banca Centrale Europea e tutte le banche centrali appartenenti al SEBC chiedendo loro come avessero organizzato le funzioni del *Data Protection Officer* (l'acronimo inglese differisce da quello italiano e questo fatto non contribuisce certo alla chiarezza), riscontrando una convergenza verso un'evidenza strutturale autonoma e un numero di risorse dedicate che oscilla fra le 3 e le 4 unità. Abbiamo anche registrato casi – Banca di Spagna, Bafin e Banca di Olanda – in cui i compiti del RPD (o DPO) sono associati con le funzioni di *compliance* e di trasparenza, in piena analogia con il nostro assetto; inoltre, alcune banche centrali (Banco del Portogallo, Banca Nazionale di Bulgaria, Banca Nazionale di Romania) riconducono l'attività del DPO agli Uffici di Gabinetto del Governatore e anche questa soluzione presenta forti analogie con la nostra, dato che alla mia figura sono assegnati anche compiti di alta consulenza al Direttorio per le relazioni istituzionali.

Ci tengo a sottolineare che, in generale, la *survey* che abbiamo promosso presso le altre banche centrali ci ha rivelato che i compiti del DPO in Europa sono ovunque cresciuti e hanno richiesto di potenziare le risorse dedicate e individuare modalità organizzative nuove, quale quella di istituire "referenti" per la protezione dei dati nelle diverse articolazioni aziendali allo scopo di concorrere all'osservazione dei trattamenti e alla gestione di *data breach* e di istanze di accesso.

Il rilievo che hanno assunto le tematiche afferenti alla protezione dei dati personali nell'attività delle banche centrali dell'Eurosistema è icasticamente espresso dalle reazioni del pubblico al progetto dell'euro digitale (*euro digital currency*). La consultazione pubblica lanciata dalla Banca Centrale Europea il 12

ottobre 2020 e terminata il 12 gennaio scorso ha ricevuto oltre 8.200 risposte, il numero più elevato mai registrato per un'iniziativa del genere della BCE. La vasta maggioranza dei partecipanti è risultata costituita da privati cittadini (94%), mentre la parte restante da professionisti, fra cui banche, fornitori di servizi di pagamento, esercenti e società tecnologiche. È emerso che cittadini e professionisti europei si aspettano da una valuta digitale innanzitutto la tutela della *privacy* (su cui converge il 43% delle risposte), seguita dalla sicurezza (18%). Come ha rilevato in un'intervista al *Financial Times* il membro italiano del *Board* della BCE, Fabio Panetta, il fatto che a gestire la valuta digitale sia la banca centrale assicura una migliore protezione della *privacy*, dato che non vi sono interessi commerciali da perseguire trattando i dati degli utenti.

Nello svolgimento dell'attività istituzionale della Banca d'Italia, come del resto per le altre Autorità, si ripropone spesso il *trade off* fra l'esigenza di esercitare i poteri di cui dispone che, per conseguire finalità pubbliche di rilievo primario, prevedono in alcuni casi una forte limitazione del diritto alla riservatezza e quella di garantire la tutela della *privacy* di cittadini e imprese con i quali viene in contatto.

I casi più significativi in cui siamo chiamati a ricercare un complicato equilibrio fra queste due esigenze apparentemente confliggenti riguardano:

- le sanzioni comminate per violazioni delle norme in materia bancaria e finanziaria, per cui la pubblicazione del destinatario e degli estremi del provvedimento (anche persona fisica) assolve a finalità principalmente afflittive, connesse con il profilo della reputazione;

- l'accesso alla centrale dei rischi, un archivio dati che, per garantire una visione d'insieme dei debiti di famiglie e imprese verso il sistema bancario, permette agli intermediari la conoscenza della "storia creditizia" dei singoli soggetti censiti, a determinate condizioni;

-gli obblighi informativi nei confronti del mercato nell'esercizio della vigilanza bancaria, che possono estendersi ad aspetti personali riservati (l'onorabilità espressa dal coinvolgimento in procedimenti giudiziari e la capacità economica) e informazioni sensibili, elementi essenziali nelle valutazioni delle nostre strutture interne, ma molto delicati per la capacità di influenzare le scelte dei risparmiatori e l'attenzione del pubblico;

- la collaborazione con altre autorità, che richiede spesso lo scambio di informazioni molto riservate;

- le attività connesse con lo svolgimento di concorsi pubblici, che impongono il trattamento di dati riservati (come anche gli appalti e le procedure di evidenza pubblica);

- le richieste di accesso agli atti dei procedimenti, sempre più frequenti, da parte di enti portatori di interessi diffusi e per attività di cronaca o approfondimento giornalistico.

È chiaro – e non potrebbe essere altrimenti – che la ricerca del delicato equilibrio fra le esigenze antagoniste a cui ho fatto riferimento non può prescindere dalla puntuale applicazione delle norme e dei principi su cui si regge la normativa *privacy*, quali il rigoroso accertamento della base giuridica del trattamento, la minimizzazione dei dati censiti, la definizione di termini certi di cancellazione dei dati dagli archivi.

A monte di questa attività si pone l'annoso problema dell'adeguato e tempestivo coinvolgimento del RPD, la cui consultazione sulle questioni di protezione dei dati da parte del Titolare o del Responsabile del trattamento oppure dalle strutture interne deputate al trattamento dei dati, pur prevista dalle norme, richiede una puntuale declinazione applicativa. Non credo sia un problema che solo noi avvertiamo, sul quale stiamo ragionando: le prassi e la buona volontà dei singoli non sempre sono sufficienti; occorrono regole chiare che rendano la modalità di consultazione effettive e cogenti.

Il Documento di indirizzo sul RPD in ambito pubblico diffuso dal Garante pochi giorni fa interviene sulla questione suggerendo buone pratiche, tra le quali:

- l'individuazione di una figura interna, adeguata per posizione e competenze, che funga da punto di riferimento per il RPD, con il quale quest'ultimo possa interloquire costantemente, al fine di ricevere gli elementi per lo svolgimento dei propri compiti. Sono portato a ritenere che questa indicazione debba essere declinata prevedendo una figura del genere in ciascuna delle articolazioni organizzative, non diversamente da ciò che abbiamo riscontrato in alcune banche centrali nella *survey* condotta nell'ambito dell'Eurosistema;
- la condivisione con tale figura di un'agenda attraverso la quale fissare momenti di dialogo con una congrua periodicità e formulare proposte sulla *compliance* aziendale;
- la proceduralizzazione di forme di partecipazione consultiva tipica del RPD (DPIA, *data breach*) e il suo coinvolgimento nelle iniziative di formazione sulla *privacy*.

Un altro aspetto sul quale intendo richiamare l'attenzione riguarda lo scambio di informazioni con altre Autorità e Amministrazioni pubbliche, che di recente si è intensificato per noi, non soltanto con riferimento ai tradizionali interlocutori con cui condividiamo funzioni di controllo (Consob, Ivass, Guardia di Finanza etc.). Nelle circostanze eccezionali determinate dall'emergenza pandemica abbiamo infatti messo a disposizione, come ben sa il dott. Villanacci, le metodologie di analisi statistica che utilizziamo in campo economico alle Strutture centrali (in primis l'Istituto Superiore di Sanità) che studiavano le modalità di diffusione del virus, definendo specifici protocolli per la condivisione dei dati sanitari.

Ricordo che la comunicazione fra titolari che effettuano trattamenti di dati personali per l'esecuzione di un compito di interesse pubblico o connesso con l'esercizio di pubblici poteri è ammessa se prevista da disposizioni di legge o di regolamento che ne disciplinino anche il contenuto o, in mancanza, se assentita dal Garante con la procedura di silenzio-assenso nel termine di 45 giorni. Il principio di minimizzazione dei dati, richiamato espressamente nel caso di trattamento di dati per finalità di ricerca scientifica o a fini statistici, trova attuazione non soltanto nella raccolta dei dati strettamente necessari, ma anche nell'adozione delle misure di protezione che assicurino un accesso ai dati correlato all'uso che se ne fa (ad es. la pseudonimizzazione in funzione dell'analisi statistica o economica propria del trattamento).

Da ultimo, vorrei concludere questi miei brevi spunti di riflessione richiamando ancora una volta il documento di indirizzo del Garante su designazione, posizione e compiti del RPD in ambito pubblico. Premesso che lo stiamo analizzando in profondità ed è

ancora presto per trarre conclusioni certe su eventuali implicazioni operative e organizzative, mi sembra che alcune indicazioni – in termini di coinvolgimento preventivo, messa a disposizione di risorse qualificate e dedicate, linea di riporto diretta al Vertice, inquadramento in posizione di autonomia e di indipendenza, autorevolezza della figura – trovano la Banca d'Italia "sulla buona strada".

Ancora lontana da un livello accettabile per un moderno Paese occidentale come il nostro è tuttavia la comunicazione in materia di *privacy*. Il messaggio che passa nell'opinione pubblica nostrana è che la normativa a protezione dei dati personali ha una dimensione prettamente burocratica, fatta di cavilli che servono soltanto a tutelare le aziende nei confronti dei consumatori, costretti a rilasciare consensi più o meno consapevoli ogni volta che viene invocato il tema della *privacy* per accedere a un servizio o per acquistare un prodotto.

L'"uomo della strada" non ha una chiara consapevolezza delle importanti finalità a cui è preordinata la normativa a protezione dai dati personali, che concorre a tutelare la sua libertà e rappresenta oggi un pilastro fondamentale dei sistemi democratici. Farne oggetto di un'azione educativa fin dalla scuola primaria è un fatto di civiltà; diffonderne la conoscenza attraverso iniziative ispirate al modello dell'educazione finanziaria che le banche centrali hanno lanciato circa un ventennio fa potrebbe essere il modo per consolidare quella cultura della legalità tanto spesso evocata in questo Paese.