DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

La concezione funzionale di titolare e responsabile del trattamento

Riflessi nei rapporti di outsourcing bancario e finanziario

8 Luglio 2026

Aurora Agostini, Partner, Lexia

DB non solo diritto bancario

Aurora Agostini, Partner, Lexia

Aurora Agostini

Aurora Agostini è partner responsabile del team Data & Technology Innovation di Lexia Avvocati. Assiste clienti in tutti i settori del diritto dell'informatica, della proprietà intellettuale e delle nuove tecnologie, con un'ampia competenza sugli aspetti della protezione dei dati e della privacy. La sua attività si concentra sulle misure di compliance, come le procedure e la documentazione richieste dal GDPR, la valutazione della base giuridica del trattamento, la conformità digitale (ad esempio i cookie), le politiche sulla privacy, le risposte ai reclami e l'esercizio dei diritti, i trasferimenti transfrontalieri di dati.

Avvocati

Lexia

LEXIA LAW | TAX | INNOVATION

1. Premessa: la qualificazione dei ruoli privacy come problema di governance del dato

Nel contesto bancario e finanziario, la protezione dei dati personali ha superato da tempo l'ambito della semplice predisposizione di informative e raccolta consensi, ed è diventata una questione cruciale di *governance* del dato. Questo implica un insieme complesso di regole, ruoli, responsabilità, controlli e processi attraverso cui un'organizzazione gestisce i dati lungo tutto il loro ciclo vitale.

L'esternalizzazione delle funzioni ICT, la digitalizzazione dei servizi di pagamento, l'adozione di soluzioni *cloud* e l'integrazione con piattaforme *fintech* hanno aumentato significativamente il numero degli attori coinvolti nel trattamento dei dati clienti: *cloud provider*, *outsourcer* informatici, *processor* di pagamenti, fornitori KYC/AML, *provider* antifrode, sistemi per *credit scoring* e *data analytics* sono solo alcuni esempi.

In tale contesto complesso, stabilire chi sia titolare o responsabile del trattamento non è affatto scontato; tuttavia, da questa definizione dipendono gli obblighi legali attribuiti ai vari attori nonché la struttura contrattuale adottata. Spesso si ricorre a una prassi comune in cui il fornitore viene designato come "responsabile del trattamento" ex art. 28 GDPR senza considerare le reali funzioni svolte, ma si tratta di un automatismo che non resiste all'esame della concezione funzionale proposta dall'EDPB, ed accolta dalla giurisprudenza.

2. Il quadro normativo

Le coordinate normative sono note, ma conviene richiamarle nella prospettiva che qui interessa. L'art. 4, n. 7, GDPR definisce titolare del trattamento la persona fisica o giuridica che, "singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento"; il successivo n. 8 definisce responsabile il soggetto che "tratta dati personali per conto del titolare". La distinzione non è meramente classificatoria: sul titolare grava, ai sensi dell'art. 24, il principio di *accountability*, in forza del quale egli non deve soltanto rispettare il Regolamento, ma deve essere in grado di dimostrare di averlo rispettato, mediante misure tecniche e organizzative adeguate e documentate.

Completano il quadro l'art. 26, che disciplina la contitolarità quando due o più soggetti determinano congiuntamente finalità e mezzi; l'art. 28, che regola il rapporto titolare-responsabile e ammette il

vedi l'articolo online

ricorso a sub-responsabili previa autorizzazione, scritta e specifica o generale, del titolare; l'art. 32, che ripartisce tra titolare e responsabile gli obblighi di sicurezza; e l'art. 82, che costruisce il regime risarcitorio in funzione del ruolo: il titolare risponde dei danni cagionati dal trattamento non conforme, mentre il responsabile risponde solo se non ha adempiuto gli obblighi che il Regolamento pone specificamente a suo carico o se ha agito in difformità dalle istruzioni ricevute.

È evidente, allora, che l›errata qualificazione di un soggetto della catena non costituisce un vizio formale, ma altera l›intera allocazione di obblighi e responsabilità: chi è stato designato responsabile, ma opera di fatto come titolare, risponde come titolare; e il titolare che ha abdicato alle proprie prerogative decisionali non può opporre la designazione contrattuale per esimersi dai propri obblighi.

3. La concezione funzionale secondo l'EDPB e il Garante

La base teorica della questione sono le Linee guida 07/2020 dell'EDPB su titolare e responsabile del trattamento e su come allocare le responsabilità in base al ruolo effettivamente svolto: lo *status* di un soggetto è determinato da ciò che viene effettivamente fatto in una situazione particolare, non dalla designazione formale nel contratto. Ci sono "elementi fattuali" nelle assegnazioni di ruolo e come tali le assegnazioni di ruolo non sono negoziabili, come dice l'EDPB.

Da questa prospettiva discendono quattro corollari operativi. Primo: la qualifica non è liberamente disponibile dalle parti, sicché la clausola che designa il fornitore come responsabile non vale a renderlo tale se i fatti dimostrano il contrario. Secondo: la designazione contrattuale conserva un valore indiziario e organizzativo, ma non è decisiva. Terzo: l'analisi deve essere condotta trattamento per trattamento, non per rapporto contrattuale o per soggetto. Quarto: il medesimo soggetto può essere titolare per talune attività, responsabile per altre e sub-responsabile per altre ancora, all'interno dello stesso rapporto negoziale.

Sul piano dei criteri, l'EDPB distingue tra mezzi essenziali del trattamento - quali i tipi di dati trattati, le categorie di interessati, la durata della conservazione, i destinatari - la cui determinazione è riservata al titolare, e mezzi non essenziali, di carattere tecnico-organizzativo, la cui scelta può essere rimessa al responsabile. Rilevante è altresì la precisazione per cui la titolarità non presuppone l'accesso ai dati: può essere titolare anche chi non compie materialmente alcuna operazione di trattamento, purché eserciti un'influenza determinante su finalità e mezzi essenziali, come confermato dalla Corte di giustizia nella sentenza 5 dicembre 2023, causa C-683/21.

L'impostazione è stata pienamente recepita dal Garante per la protezione dei dati personali, che, da ultimo con provvedimento dell'11 settembre 2025, ha ribadito che ai fini dell'individuazione del ruolo "è essenziale esaminare sul piano sostanziale e non formale le attività in concreto svolte" dai soggetti coinvolti.

4. La giurisprudenza di legittimità: dal formalismo alla funzione

La Corte di cassazione ha progressivamente fatto proprio il criterio sostanziale, in linea con l'EDPB e la Corte di giustizia.

Con l'ordinanza 23 luglio 2021, n. 21234, la Suprema Corte ha individuato nell'autonomo potere decisionale l'elemento qualificante della titolarità: il soggetto preposto al trattamento su incarico altrui che si discosti dalle istruzioni ricevute, esercitando scelte proprie su finalità e modalità, assume in concreto la veste di titolare, con le connesse responsabilità, a nulla rilevando l'originaria configurazione del rapporto.

Con l'ordinanza 21 settembre 2023, n. 26969, resa in materia di sistemi di geolocalizzazione, la Corte ha precisato che la titolarità non dipende necessariamente dall'accesso effettivo ai dati, bensì dalla loro disponibilità e dalla possibilità di gestirli: la stessa consegna delle credenziali di accesso al sistema può costituire indice del trasferimento del potere decisionale sulle finalità e modalità del trattamento. Viene così censurata la prospettiva, formalistica, che identifica il titolare in chi materialmente "detiene" la tecnologia anziché in chi governa il trattamento.

La sentenza 18 dicembre 2023, n. 35256, ha affrontato la catena titolare-responsabile-sub-responsabile in un rapporto di subfornitura di servizi (gestione di parcometri), affermando che il trattamento svolto da un soggetto non formalmente designato quale sub-responsabile è privo di condizioni di liceità, senza che la carenza possa essere supplita da pattuizioni privatistiche tra committente e subfornitore, né sanata da designazioni successive all'avvio del trattamento. Il rigore della pronuncia si spiega proprio in chiave funzionale: la formalizzazione ex art. 28 non è un adempimento burocratico, ma lo

strumento che rende trasparente e controllabile la catena decisionale.

Da ultimo, l'ordinanza 15 ottobre 2025, n. 27558, in tema di Fascicolo sanitario elettronico, ha cassato la decisione di merito che aveva individuato i ruoli sulla base di atti formali — il piano di progetto e l'atto di nomina del responsabile — senza verificare quali soggetti, in base alla normativa di settore, determinassero finalità e mezzi del trattamento. La pronuncia è significativa per un duplice profilo: da un lato, conferma che gli atti di nomina non possono prevalere sull'assetto sostanziale dei poteri decisionali; dall'altro, chiarisce che la titolarità può derivare direttamente dalla disciplina settoriale che attribuisce a un soggetto determinate finalità e i relativi mezzi.

Si tratta di un rilievo di immediato interesse per il settore bancario e finanziario, dove numerosi trattamenti — antiriciclaggio, segnalazioni di vigilanza, centrale rischi, trasparenza — trovano fonte e conformazione nella normativa di settore, che concorre a radicare in capo all'intermediario, o ad altri soggetti della filiera, una titolarità *ex lege* insensibile alle qualificazioni contrattuali.

5. Le ricadute sui rapporti di outsourcing

Questi principi devono essere verificati in ogni fase della catena degli intermediari che determina le finalità e i mezzi essenziali e chi lavora per altri, e chi ha un certo margine decisionale autonomo. Alcuni degli esempi ricorrenti dimostrano la loro portata.

Il fornitore di *cloud* è solitamente il responsabile, ma la qualificazione deve essere misurata rispetto alle decisioni del fornitore sulla localizzazione e telemetria, analisi dei dati, riutilizzo dei dati per miglioramento del servizio o addestramento del modello; dove queste attività servono ai propri scopi del fornitore, per loro questo può essere considerato un titolare autonomo.

Il *processor* di pagamenti può essere responsabile delle attività tecniche svolte dall'intermediario ed è autonomo nel trattamento come è nel campo della disciplina che lo riguarda maggiormente: sicurezza, prevenzione delle frodi, antiriciclaggio e gestione dei reclami.

E ancora, il fornitore di servizi KYC/AML: se esegue solo controlli per la banca, allora è responsabile; se ha i propri database e arricchimenti, *scoring* per più clienti secondo la propria logica, è un titolare autonomo o contitolare.

Anche nel contesto antifrode e *cybersecurity*, i mezzi essenziali sono riservati al titolare bancario e i mezzi non essenziali sono lasciati alla discrezione tecnica del fornitore. Un margine decisionale troppo elevato e molto superiore al livello esecutivo tecnico del fornitore di servizi fa cambiare la qualificazione. Come gruppo bancario, l'azienda che fornisce servizi intercompany (ICT, risorse umane, compliance, marketing) non è automaticamente responsabile, ma a seconda del servizio e delle decisioni prese nel processo, può essere responsabile, contitolare o titolare autonomo poiché non esiste un'esenzione intra-gruppo nel GDPR.

La piattaforma CRM o di automazione del *marketing* è responsabile dell'invio dei messaggi su istruzioni della banca, ma è un titolare autonomo se utilizza i dati per *benchmarking*, arricchimento, proprio *profiling* o sviluppo autonomo del servizio.

Un discorso a sé merita, infine, l'*open banking*: il prestatore terzo che accede ai conti su richiesta del cliente (AISP o PISP) non opera "per conto" della banca, ma persegue finalità proprie sulla base di un autonomo rapporto con l'interessato, e va dunque qualificato come titolare autonomo, quantunque il flusso di dati transiti dalle interfacce dell'intermediario E questo è forse l'esempio più chiaro di come la responsabilità negoziale o regolatoria di un soggetto nella catena di fornitura non determini di per sé il loro ruolo in materia di *privacy* nella catena di fornitura.

6. Presidi contrattuali e organizzativi

A livello operativo, la concezione funzionale richiede agli intermediari di adottare un metodo, ancor prima di un insieme di clausole: l'errore che non si dovrebbe commettere è procedere dagli accordi contrattuali al trattamento; il percorso corretto dal trattamento effettivo allo strumento negoziale che li rappresenta è passare dal trattamento alla negoziazione.

Occorre mappare i trattamenti per finalità e flussi di dati; verificare il ruolo di ciascun soggetto per ciascun trattamento; scegliere di conseguenza lo strumento negoziale appropriato, distinguendo tra *data processing agreement* ex art. 28, accordo di contitolarità ex art. 26 e regolamentazione dei rapporti tra titolari autonomi, senza ricorrere in via automatica al DPA. Va poi presidiata la catena dei sub-respon-

sabili - intendendosi per sub-responsabile il soggetto incaricato dal responsabile di svolgere, per conto del titolare, specifiche attività di trattamento, previa autorizzazione del titolare e con obblighi sostanzialmente equivalenti a quelli del responsabile — la cui mancata formalizzazione, come chiarito da Cass. n. 35256/2023, travolge la stessa liceità del trattamento.

Le salvaguardie della privacy devono poi allinearsi con le normative sull'*outsourcing* ICT e il regolamento DORA in modo che il registro dei trattamenti, il registro delle informazioni ai sensi dell'Articolo 28 DORA e gli accordi contrattuali non descrivano catene di fornitura divergenti. Pertanto, si dovrà discutere il riutilizzo dei dati, i log, l'analisi, la formazione dei sistemi di intelligenza artificiale e altre finalità del trattamento dei dati (anche personali) del fornitore, che oggi sono i principali motori del passaggio dalla qualifica di titolare a titolare indipendente. Le salvaguardie sono rappresentate da istruzioni scritte, diritti di audit, obblighi di assistenza, gestione delle violazioni dei dati e la definizione delle misure di sicurezza ai sensi dell'Articolo 32 GDPR.

7. Conclusioni: la forma segue la funzione

EDPB, Garante e Cassazione concordano su un punto: i ruoli *privacy* sono qualifiche sostanziali, che il contratto deve fotografare, non costruire. Nel settore bancario e finanziario, dove l'esternalizzazione tecnologica porta a qualifiche tecnicamente corrette ma sostanzialmente errate, la domanda che dovremmo porci non è "cosa abbiamo scritto nel contratto?" ma "chi decide veramente perché e come vengono trattati i dati?".

Solo a valle di questa analisi la **contrattualistica *privacy*** può essere correttamente impostata; in caso contrario, essa non alloca i rischi, ma si limita a occultarli fino alla prima verifica ispettiva o alla prima azione risarcitoria. La forma, insomma, segue la funzione: mai il contrario.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it