IL TRATTAMENTO DEI DATI CORRELATI AI SERVIZI DI PAGAMENTO

2 febbraio 2026

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Giovanni Lombardi
Associate

Alessandro Carlini
Associate

Beatrice Pedroni
Associate

La rivoluzione dell'*open banking* indotta dalla PSD2 ha trasformato i servizi di pagamento in un'infrastruttura informativa diffusa, nella quale l'operazione finanziaria è, al contempo, processo transazionale e flusso di dati personali.

L'accesso regolato ai conti di pagamento mediante interfacce standardizzate, la proliferazione di prestatori terzi e l'innalzamento degli standard di sicurezza (SCA e comunicazioni sicure) hanno moltiplicato i punti di contatto fra disciplina bancaria e protezione dei dati, rendendo evidente che il pagamento digitale è, prima ancora che un trasferimento di fondi, un trattamento di dati. In questo contesto, l'equilibrio tra esigenze di innovazione, sicurezza del sistema e tutela dei diritti degli interessati non può essere ricercato attraverso letture settoriali, ma richiede un coordinamento sistematico fra GDPR e PSD2, come ricostruito dalle Linee guida 06/2020 dell'EDPB, e una traduzione architetturale dei principi di minimizzazione, trasparenza, responsabilizzazione e sicurezza.

Il presente contributo propone una lettura integrata del quadro regolatorio, soffermandosi su cinque profili: il necessario coordinamento tra PSD2 e GDPR; la distinzione concettuale fra "consenso esplicito" e categorie particolari di dati; il trattamento dei dati dei c.d. "taciti interessati"; l'applicazione concreta dei principi di protezione dei dati nei processi e nelle architetture dei prestatori; l'uso dei dati per finalità antifrode, ivi inclusa l'analisi comportamentale e il monitoraggio delle transazioni.

▼ ▼ ▼

IL NECESSARIO COORDINAMENTO FRA GDPR E PSD2: LE LINEE GUIDA EDPB

Il punto di partenza è normativo: l'articolo 94 della PSD2 impone che ogni trattamento di dati personali ai fini della direttiva avvenga in conformità al GDPR e alle pertinenti norme in materia di sicurezza, ribadendo quanto già anticipato dai considerando 89 e 93. Ne discende che la PSD2 non introduce un autonomo regime di liceità dei trattamenti, né rappresenta una *lex specialis* idonea a derogare al GDPR; piuttosto, essa disegna il perimetro soggettivo e oggettivo dell'accesso regolato ai conti e, contestualmente, rinvia al GDPR per la scelta della base giuridica e per l'osservanza dei principi di cui all'articolo 5.

L'EDPB, nelle Linee guida 06/2020, chiarisce che, per la prestazione del servizio in senso stretto (accesso al conto, avvio dell'operazione, gestione tecnica dell'istruzione di pagamento), la base giuridica tipica è l'articolo 6, paragrafo 1, lettera b), GDPR (necessità contrattuale). Tale base giuridica opera tanto per i prestatori "tradizionali" (ASPSP) quanto per gli operatori introdotti dalla PSD2 (AISP e PISP), a condizione che il trattamento sia circoscritto a quanto strettamente necessario per erogare il servizio espressamente richiesto dall'utente. La direttiva, peraltro, introduce specifiche cautele di contesto: gli articoli 66 e 67 limitano in modo rigoroso la raccolta e il riuso dei dati da parte di PISP e AISP, vietando qualsiasi utilizzo per finalità ulteriori rispetto alla prestazione del servizio. La prevenzione delle frodi, richiamata dall'articolo 94, non costituisce di per sé una base autonoma di liceità nel senso del GDPR, ma può fondarsi, caso per caso, su un obbligo legale (ad es. normativa antiriciclaggio e di vigilanza) o su un legittimo interesse debitamente bilanciato e documentato. In questa prospettiva, la PSD2 "abilita" l'accesso ai dati nei limiti del servizio regolato; il GDPR "abilita" il trattamento, definendone condizioni, limiti, garanzie e responsabilità. La giurisprudenza della Corte di giustizia, valorizzando trasparenza e tracciabilità (si pensi alla sentenza Pankki S[1] in tema di diritto di accesso ai log di consultazione), conferma che i dati bancari e i relativi metadati di accesso sono dati personali a pieno titolo e che le garanzie di cui agli articoli 12–15 GDPR non sono recessive nel settore dei pagamenti. Ne deriva, sul piano operativo, l'esigenza di un disegno di governance che saldi i requisiti regolamentari PSD2 con i principi e gli obblighi del GDPR, evitando tanto il formalismo documentale quanto il tecnicismo deresponsabilizzante.

▼▼

L'art. 94 PSD2 non introduce una base giuridica autonoma:

il trattamento resta integralmente soggetto al GDPR

LE DIVERSE NOZIONI DI "CONSENSO ESPLICITO" E "DATI SENSIBILI"

Il lessico comune tende a sovrapporre nozioni che, nel diritto positivo, hanno funzioni distinte.

Anzitutto, il "consenso esplicito" richiesto dall'articolo 94, paragrafo 2, PSD2 non coincide con il consenso quale base giuridica ai sensi del GDPR. L'EDPB precisa che il consenso PSD2 ha natura contrattuale-regolatoria: è la dichiarazione con cui l'utente autorizza l'accesso ai dati del conto e il loro trattamento/conservazione in quanto necessari alla prestazione del servizio di pagamento richiesto; tale consenso non sostituisce, né integra, le basi di liceità previste dall'articolo 6 GDPR.

Di regola, per l'esecuzione del servizio, la base giuridica resta l'articolo 6, paragrafo 1, lettera b); il consenso GDPR (articolo 6, paragrafo 1, lettera a)) può venire in rilievo solo per finalità ulteriori, non necessarie alla prestazione (es. funzionalità

[1] CGUE, sentenza Pankki S (C-579/21).

opzionali, marketing, profilazioni non strettamente tecniche), e comunque alle stringenti condizioni di validità e dimostrabilità di cui agli articoli 4, 7 e ai considerando 32 e 42. Sul piano sostanziale, il consenso PSD2 delimita "chi può accedere a cosa, per quale servizio e per quanto tempo", mentre il consenso GDPR, ove utilizzato, legittima specifiche finalità di trattamento, revocabili senza pregiudizio e in assenza di asimmetrie tali da inficiare la libertà dell'assenso.

Ugualmente importante è distinguere tra "**dati sensibili relativi ai pagamenti**" nel significato funzionale della PSD2 e "**categorie particolari di dati**" nel senso dell'articolo 9 GDPR. La PSD2 qualifica come "sensibili" le informazioni idonee a commettere frodi, incluse le credenziali di sicurezza personalizzate, e disciplina la loro protezione anche rispetto alla capacità di AISP e PISP di richiederle o conservarle. Il GDPR, invece, qualifica come "particolari" le categorie tassative elencate all'articolo 9 (dati sanitari, convinzioni religiose o sindacali, orientamento sessuale, dati biometrici, ecc.), sottoponendone in via generale a divieto il trattamento salvo specifiche deroghe.

▼▼

La "sensibilità" PSD2 è funzionale alla sicurezza del pagamento e non coincide con le categorie particolari di dati ex art. 9 GDPR

I dati di pagamento, in quanto tali, non rientrano *ex se* nell'articolo 9; nondimeno, singole transazioni possono rivelare indirettamente informazioni appartenenti a tali categorie (pagamenti a cliniche, donazioni politiche, contributi a confessioni religiose), attivando il presidio dell'articolo 9 e l'esigenza di un esplicito consenso ai sensi dell'articolo 9, paragrafo 2, lettera a), o di altra base derogatoria applicabile.

Da ciò discende, in concreto, l'obbligo per i prestatori di progettare i flussi informativi e gli schemi dati in modo da minimizzare l'esposizione a tali informazioni inferenziali, limitando – ove possibile – la raccolta e la conservazione di campi descrittivi sensibili, e adottando soluzioni tecniche (filtri, mascheramenti, esclusioni selettive) che impediscano la circolazione di categorie particolari, specie rispetto ai dati di terzi.

IL TRATTAMENTO DEI DATI DEL "TACITO INTERESSATO"

Nell'ecosistema dei pagamenti, l'interessato non coincide sempre con il cliente contrattuale del prestatore: beneficiari di bonifici, controparti di operazioni, soggetti menzionati nelle causali costituiscono "taciti interessati" (*silent parties*) i cui dati vengono trattati senza che esista un rapporto diretto con l'operatore che esegue o abilita l'operazione.

Le Linee guida EDPB riconoscono la legittimità di tali trattamenti entro confini puntuali. In primo luogo, la base giuridica idonea è, di regola, il legittimo interesse del titolare o di terzi (articolo 6, paragrafo 1, lettera f)), consistente nel dare esecuzione al contratto di servizi di pagamento instaurato con l'utente e nel

garantire il funzionamento regolare e sicuro del sistema.

Il trattamento dei dati dei terzi si fonda, di regola, sul legittimo interesse debitamente bilanciato

Questa base non opera automaticamente: è necessario un bilanciamento documentato che verifichi la stretta necessità del trattamento, la prevedibilità per il terzo e l'adozione di misure adeguate a tutelarne diritti e libertà, incluso il divieto di riuso per finalità ulteriori.

In secondo luogo, il principio di trasparenza si declina qui mediante l'informativa ex articolo 14 GDPR: non è realistico, né proporzionato, pretendere una comunicazione individuale a ogni controparte potenziale; è invece richiesto che i prestatori mettano a disposizione un'informativa dedicata ai taciti interessati, pubblicata in modo facilmente accessibile e redatta con riferimento a categorie di dati, finalità strettamente connesse all'operazione (esecuzione, obblighi normativi, prevenzione frodi), basi giuridiche e tempi di conservazione, nonché canali per l'esercizio dei diritti. In terzo luogo, l'ulteriore trattamento dei dati dei taciti interessati è consentito solo nei limiti derivanti da obblighi legali specifici (ad esempio, misure AML/CFT) o da un consenso valido ove pertinente, fermo il divieto di utilizzi incompatibili con la finalità originaria.

Questa impostazione realizza l'equilibrio fra la possibilità per l'intermediario di eseguire l'operazione senza oneri inibenti e la tutela del terzo, il cui perimetro di trattamento è ristretto a quanto ragionevolmente prevedibile alla luce della natura dell'operazione e delle regole del sistema.

DALLA TEORIA ALLA PRATICA: MINIMIZZAZIONE, TRASPARENZA, RESPONSABILIZZAZIONE E SICUREZZA

La conformità, nel dominio dei pagamenti, non è mai meramente documentale: è anzitutto progettazione di processi e sistemi.

Il **principio di minimizzazione** impone di determinare ex ante quali categorie di dati siano davvero necessarie per ciascun servizio e per ciascun flusso: identificativi, IBAN, saldo, storico delle transazioni, metadati di accesso e di dispositivo, causali. Per i servizi di informazione sui conti, l'accesso deve restare confinato ai conti designati e al periodo strettamente necessario; per i servizi di disposizione di ordini, la raccolta non può eccedere i dati indispensabili alla specifica esecuzione. Questa determinazione deve riflettersi nelle specifiche delle API, nei profili di autorizzazione, nelle politiche di logging e retention, secondo la logica di privacy by design e by default dell'articolo 25.

Il **principio di trasparenza** richiede informative multilivello, chiare e specifiche, che distinguano ruoli e responsabilità dei diversi attori (ASPSP, AISP, PISP), chiariscano le basi giuridiche per finalità "core" e "ulteriori", espongano gli effetti delle misure

antifrode e dei controlli automatizzati, e indichino con precisione le logiche essenziali delle decisioni che producano effetti giuridici o analogamente significativi. La Corte di giustizia, nel caso Pankki S, ha ribadito il diritto dell'interessato a conoscere le circostanze della consultazione dei propri dati (date, ragioni, categorie di destinatari), pur escludendo la necessità di rivelare l'identità nominativa dei dipendenti che hanno effettuato l'accesso, confermando l'esigenza di sistemi di audit trail granulari e verificabili.

La **responsabilizzazione (*accountability*)** integra e salda gli altri principi, esigendo mappature accurate dei trattamenti, separazione delle finalità (esecuzione, sicurezza antifrode, adempimenti legali, finalità opzionali), analisi di necessità e proporzionalità, valutazioni d'impatto quando ricorrano trattamenti su larga scala o monitoraggi sistematici, nonché governance dei rapporti di contitolarità o contenziosa allocazione dei ruoli tra prestatori.

La **sicurezza**, infine, è il luogo dell'integrazione più stretta tra PSD2 e GDPR: l'articolo 32 GDPR impone misure adeguate al rischio; l'RTS sulla strong customer authentication e sulle comunicazioni sicure pretende meccanismi di autenticazione a fattori multipli, segregazione degli ambienti, gestione rigorosa delle credenziali e, soprattutto, sistemi di monitoraggio delle transazioni idonei a individuare pattern anomali.

La coerenza fra sicurezza e protezione dei dati si misura nella capacità di calibrare gli strumenti di monitoraggio sul rischio, contenendone la portata ai soli dati e alle sole metriche necessarie, con tempi di conservazione ridotti, separazione logica e organizzativa dei dataset antifrode rispetto ad altri scopi, e controlli di accesso strettamente need-to-know.

USO DEI DATI PER INDIVIDUARE LE FRODI: ANALISI COMPORTAMENTALE E MONITORAGGIO DELLE TRANSAZIONI

La prevenzione delle frodi è un interesse sistemico e un requisito strutturale dei servizi di pagamento; senza trattamenti antifrode efficaci, il sistema non reggerebbe.

Ciò, tuttavia, non legittima approcci illimitati o generalizzati. La PSD2 riconosce la liceità del trattamento ai fini antifrode, ma la sua attuazione deve trovare fondamento, nel senso del GDPR, in obblighi legali specifici ovvero in un legittimo interesse del prestatore proporzionato e debitamente bilanciato.

L'evoluzione degli strumenti ha condotto oltre le regole statiche verso modelli basati su analisi comportamentale e apprendimento automatico: monitoraggio continuo dei pattern transazionali, correlazione spazio-temporale degli accessi,

I modelli antifrode costituiscono spesso profilazione ai sensi dell'art. 4(4) GDPR

rilevazione di sequenze anomale (test *micro-transaction*, *escalation* di importi, triangolazioni geografiche). Tali trattamenti comportano, nella maggior parte dei casi, attività di profilazione ai sensi dell'articolo 4, punto 4), e possono sfociare in decisioni automatizzate che producono effetti giuridici o significativamente analoghi (blocco del pagamento, richiesta di step-up di autenticazione, sospensione temporanea).

La giurisprudenza recente (casi Schufa e Dun & Bradstreet[2]) ha ampliato la sensibilità del sistema verso gli impatti delle decisioni automatizzate, esigendo presidi rafforzati: spiegazioni significative delle logiche di base, possibilità di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione, tracciabilità delle revisioni, calibrazione e audit dei modelli, periodiche verifiche di *bias* e tassi di errore.

Il principio di limitazione della finalità impedisce che i dati e i segnali raccolti per l'antifrode siano riutilizzati per scopi diversi senza una valutazione di compatibilità ex articolo 6, paragrafo 4, o senza un'autonoma base giuridica. L'accountability impone, inoltre, metriche di qualità dei modelli, conservazioni differenziate e temporalmente limitate dei dati grezzi e delle feature derivate, nonché un'architettura di segregazione che eviti commistioni fra ambienti antifrode e domini di business.

È decisivo, in questa prospettiva, riconoscere che proporzionalità e minimizzazione non sono antitetiche all'efficacia antifrode, ma ne sono condizione: strumenti più accurati e circoscritti, con dataset pertinenti e ridotti al necessario, generano minori falsi positivi, riducono le superfetazioni informative e migliorano la protezione complessiva del sistema e degli interessati.

CONCLUSIONI

Il coordinamento tra PSD2 e GDPR, come ricostruito dall'EDPB, non è un esercizio esegetico, ma un progetto organizzativo e tecnico. La PSD2 definisce i diritti di accesso e i confini regolamentari dei servizi; il GDPR fissa le condizioni di liceità, i principi e le garanzie del trattamento. In mezzo, vivono le architetture applicative, le API, i modelli antifrode, i registri degli accessi, i flussi di informativa, i processi di gestione dei diritti, le politiche di retention e di sicurezza.

È su questo piano che si gioca l'effettività della tutela: nella capacità dei prestatori di tradurre la necessità contrattuale in perimetri informativi minimi; di distinguere con nettezza il consenso contrattuale PSD2 dal consenso GDPR; di trattare i dati dei taciti interessati entro orizzonti prevedibili e protetti; di costruire sistemi di

[2] CGUE, sentenze Schufa (C-634/21), Dun & Bradstreet (C-203/22).

sicurezza che non divengano alibi per trattamenti ultronei; di addestrare e verificare modelli antifrode trasparenti, contestabili e proporzionati.

Le imminenti riforme europee del quadro dei pagamenti (PSD3 e Payment Services Regulation) sembrano muoversi in continuità con questa linea: rafforzamento delle garanzie per gli utenti, maggiore controllo sull'accesso, vigilanza più stringente su sicurezza e prevenzione delle frodi. In tale scenario, la protezione dei dati non è un vincolo esterno al mercato dei pagamenti, ma la condizione della sua sostenibilità: il GDPR non limita l'*open banking*; lo rende possibile, affidabile e degno di fiducia.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Giovanni Lombardi

Associate

Alessandro Carlini

Associate

Beatrice Pedroni

Associate