Banking & Finance

Il settore bancario tra GDPR e PSD2

1. Il GDPR e l'impatto sul mondo bancario.

Dal 25 maggio 2018 è applicabile il Regolamento UE 679/2016 sulla protezione dei dati personali ("**GDPR**")[1]. Il GDPR si applica ai trattamenti di dati personali effettuati da soggetti stabiliti nell'Unione Europea, nonché ai trattamenti di dati personali di soggetti interessati che si trovino nell'Unione Europea, indipendentemente da dove si effettui il trattamento.

Il GDPR ha inteso bilanciare due esigenze potenzialmente in conflitto: favorire la libera circolazione dei dati personali e assicurare contestualmente la protezione di tali dati.

La nuova disciplina non costituisce dunque un ostacolo al trattamento dei dati ma – al contrario – intende assicurare che tale trattamento sia effettuato in maniera trasparente, garantendo all'interessato il diritto di essere sempre informato sull'esistenza di un trattamento avente ad oggetto dati personali che lo riguardano, nonché sulle modalità di svolgimento di tale trattamento.

Data l'ampiezza della sua portata, il GDPR è destinato ad avere, nei prossimi anni, un impatto significativo in tutti i settori in cui avviene un trattamento di dati personali.

Il **settore bancario** è uno dei settori su cui maggiore sarà l'impatto del GDPR: gli operatori bancari ([2]), nello svolgimento della propria attività, acquisiscono per ogni cliente un numero estremamente elevato di dati personali.

Questi dati, per numero e varietà, permettono all'operatore bancario di effettuare una costante attività di profilazione dei propri clienti.

La profilazione è oggetto di particolare attenzione da parte del GDPR per l'impatto che essa può avere sui diritti e le libertà degli interessati, in particolare quando eseguita con un trattamento automatizzato. Più precisamente, il GDPR prende in considerazione "***qualsiasi forma di trattamento automatizzato*** *di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le*

1 Il 19 settembre 2018 è entrato in vigore il D.lgs. 10 agosto 2018, n. 101 finalizzato all'adeguamento del D.lgs. 196/2003 (c.d. Codice Privacy) alla nuova disciplina europea. Il quadro normativo italiano della protezione dei dati risulta così articolato in tre livelli: Regolamento UE, Codice Privacy e decreto di adeguamento.

2 Con il termine "operatore bancario" si intendono tanto le banche, quanto gli istituti di pagamento, gli intermediari finanziari non bancari, i prestatori di servizi e attività d'investimento ecc.

preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

La profilazione del cliente è inscindibile dallo svolgimento dell'attività bancaria e gli operatori bancari compiono tale attività in due occasioni:

1. **nella prestazione di servizi di pagamento**: l'operatore bancario deve acquisire e archiviare tutti i dati relativi alle operazioni di pagamento del cliente, con la conseguenza di ottenere piena visione di spese, operazioni di pagamento, acquisti ecc.
   In questo modo l'operatore bancario potrebbe facilmente creare un profilo personale del cliente da inserire all'interno di determinate categorie o classi commerciali di clientela.
   Tale profilazione può essere utilizzata in primo luogo dagli operatori bancari stessi per indirizzare ad ogni cliente offerte mirate di altri servizi bancari e finanziari (*i.e*. servizi diversi dai servizi di pagamento), presumibilmente di maggiore interesse per l'interessato.
   Inoltre, i profili personali dei clienti – a condizione che siano state adottate opportune cautele al momento della raccolta dei dati – potrebbero essere ceduti a soggetti terzi che potrebbero avvalersene per proprie finalità commerciali (ad es. campagne pubblicitarie o offerte mirate);
2. **nell'attività di *scoring* del merito creditizio e nella profilazione del cliente ai sensi della normativa MIFID** per definire l'esatta tipologia di clientela (ad es. cliente retail o cliente professionale).

Tali esempi dimostrano che l'attività di profilazione non solo è intrinseca e imprescindibile all'attività bancaria, ma talvolta è addirittura imposta *ex lege* allo scopo di adempiere specifici obblighi a carico degli operatori bancari (ad es. in ambito MIFID).

Come detto, il GDPR presta particolare attenzione al tema della profilazione, perché ravvede in essa un potenziale rischio per i diritti e le libertà degli interessati e ciò a causa dell'invasività che ne può derivare per gli aspetti più personali della vita .

La scelta del legislatore europeo, in linea con la visione generale del regolamento, è quella di ammettere la profilazione, ma richiedendo alcuni accorgimenti volti ad assicurare una adeguata tutela delle persone coinvolte.

Gli obblighi che gli operatori bancari dovranno assolvere per continuare a condurre lecitamente tale attività sono, in particolare, i seguenti:

1. fare espressa menzione nell'**informativa agli interessati** ai sensi degli artt. 13 e 14 GDPR dell'esistenza di un processo di profilazione, fornendo tutte le informazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze previste di tale trattamento per l'interessato;
2. svolgere una valutazione d'impatto sulla protezione dei dati (***Data Protection Impact Assessment* – DPIA**), obbligatoria quando un trattamento, in particolare se prevede l'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso; tale valutazione è richiesta specificamente dall'art. 35 GDPR in presenza di un'attività di profilazione;

3. designare un responsabile della protezione dei dati (***Data Protection Officer* – DPO**) previsto dall'art. 37 GDPR con il compito di assistere e consigliare il titolare del trattamento (in questo caso l'operatore bancario) con riferimento a tutte le questioni relative alla protezione dei dati personali.

2. PSD2: l'ingresso di nuovi player nel settore bancario e la privacy dei clienti.

Alle complessità operative in termini di *compliance privacy* per gli operatori bancari si sommano, in parziale sovrapposizione, alcune criticità derivanti dalla nuova direttiva sui servizi di pagamento. Il 13 gennaio 2018 è stato pubblicato in Gazzetta Ufficiale il D.lgs. 15 dicembre 2017, n. 218 di recepimento della Direttiva UE 2015/2366 (c.d. **"PSD2"**) relativa ai servizi di pagamento nel mercato interno.

La PSD2 e il GDPR sembrano destinati a generare **attriti applicativi** sotto diversi profili.

La PSD2 disciplina nuovi servizi che consentiranno agli utenti dei servizi bancari e di pagamento di rivolgersi a operatori specializzati , di derivazione non bancaria, definiti "terze parti" (o *Third Parties Pro*viders – TPP), per l'esecuzione di operazioni di pagamento e altre attività connesse ai servizi di pagamento. I TPP opereranno come "intermediari virtuali" frapponendosi tra il cliente e i servizi di pagamento erogati dagli operatori bancari veri e propri.

I TPP sono, a seconda della tipologia di servizio erogato, i **PISP** (*Payment Initiation Service Provider*), gli **AISP** (*Account Information Service Provide*) e i **CISP** (*Card Issuer Credit Provider*) [3].

Il flusso di dati derivante da tutte le operazioni di pagamento effettuate si "sposta", in tal modo, dagli operatori bancari tradizionali ai TPP, i quali si frappongono tra cliente e operatore bancario e acquisiscono, al posto di quest'ultimo, tutte le informazioni relative ad una transazione (ad esempio il bene/servizio acquistato, l'identità del "professionista" che vende il bene o il servizio on-line ecc.). In questo modo, una parte dell'attività di profilazione potrà essere effettuata da questi nuovi fornitori di servizi di pagamento.

Se da un lato questo trasferimento di flussi di dati potrebbe comportare un "alleggerimento" del carico di lavoro per gli operatori bancari, dall'altro potrebbe determinare anche la perdita della

---

3 In estrema sintesi, i **TPP** sono soggetti (in forma societaria) che andranno autorizzati dalle authority di vigilanza statali (ex art. 4 della PSD2) e rappresentano la reale novità del mercato dei pagamenti digitali. Questi nuovi player avranno la possibilità di operare direttamente sui conti correnti degli utenti finali realizzando quindi una forte disintermediazione tra operatore bancario e cliente.
Il **PISP** potrà eseguire pagamenti, ordinati dal cliente-pagatore, a valere su un conto corrente aperto presso una banca; in tal modo, il cliente della banca non sarà più costretto ad avvalersi dei servizi di pagamento online della stessa banca, potendo rivolgersi a un PISP il quale avrà il diritto di accedere ai fondi del cliente presso la banca per eseguire un pagamento digitale, senza che la banca posso opporre alcun diniego.
Tramite **l'AISP**, invece, il cliente potrà avvalersi di un servizio online per ottenere informazioni consolidate (per es. saldi, elenco movimenti etc.) in relazione a uno o più conti correnti o strumenti di pagamento detenuti dall'utente presso gli operatori bancari. L'AISP permetterà di avere una visione d'insieme istantanea di tutti i conti correnti e strumenti di pagamento e, anche in questo caso, le banche non potranno negare l'accesso del TPP ai dati.
Infine, tramite il **CISP**, sarà possibile avere immediata conferma dalla banca del cliente della disponibilità di fondi per eseguire pagamenti tramite carte di pagamento emesse da soggetti terzi, che quindi non hanno alcun rapporto con la banca del pagatore. La banca sarà pertanto tenuta a confermare se sul conto del pagatore vi è disponibilità dell'importo richiesto per l'esecuzione di un'operazione di pagamento basata su carta, senza tuttavia fornire informazioni in merito al saldo disponibile.

possibilità di elaborare i dati in maniera funzionale alla promozione dell'attività bancaria, ad esempio consentendo di indirizzare al cliente offerte tendenzialmente *tailor-made*.

3. Attriti applicativi tra GDPR e PSD2.

Dal punto di vista prettamente giuridico e contrattuale, l'ingresso nel mondo del sistema dei pagamenti dei TPP determina l'esigenza di regolare su un piano contrattuale i rapporti tra questi e gli operatori del sistema bancario tradizionale.

Un primo aspetto da considerare riguarda l'accesso ai dati dell'interessato (in questo caso il cliente).

Il GDPR mira a garantire che l'interessato sia sempre adeguatamente informato sul modo in cui i suoi dati personali sono trattati, riconoscendogli tra l'altro il diritto di controllare l'accesso ai propri dati. In una diversa prospettiva, invece, i nuovi servizi disciplinati dalla PSD2 necessitano, per poter funzionare, di una più rapida interazione tra i dati a disposizione degli operatori bancari e i TPP i quali, per poter eseguire i propri servizi, hanno bisogno di poter accedere tempestivamente ai dati del cliente trattati dall'operatore bancario. La tendenza in ambito PSD2 è, pertanto, quella di rendere i dati dei clienti maggiormente accessibili ai soggetti terzi.

Per esempio, in base alla PSD2, gli operatori bancari dovranno fornire ai TPP alcuni dati dei propri clienti allo scopo di permettere ai TPP di erogare i propri servizi, a meno che tali dati non siano qualificabili come **dati sensibili relativi ai pagamenti**.

Tuttavia, a una più attenta lettura della definizione di dati sensibili relativi ai pagamenti, si nota che il legislatore comunitario non ha fornito una nozione oggettiva e univoca di dato sensibile relativo ai pagamenti e, all'atto pratico, tale concetto potrebbe finire per essere affidato alla sensibilità degli operatori bancari [4].

Questa lacuna potrebbe, da un lato, incrementare il rischio di non conformità o, al contrario, spingere gli operatori bancari ad adottare un approccio fin troppo prudente nel definire, a fini interni e operativi, la propria nozione di dato sensibile.

Diverrà quindi essenziale **definire il ruolo** di ciascuna entità coinvolta nel trattamento dei dati dei clienti (sia dal lato dell'operatore bancario che da quello del TPP) al fine di individuare per ciascuna di esse gli obblighi da rispettare.

A tal riguardo va ricordato che , l'art. 13 del GDPR impone al titolare del trattamento l'obbligo di fornire all'interessato, su richiesta di quest'ultimo, informazioni relative al trattamento dei dati personali che lo riguardano[5].

---

4 Infatti, la definizione di "dati sensibili relativi ai pagamenti" contenuta al n. 32 dell'art. 4 della PSD2 (e trasposta nella lettera q-quater del comma 1, art. 1 del D.Lgs. 11/2010) definisce tali dati come *"dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate"* aggiungendo infine che *"per l'attività dei prestatori di servizi di disposizione di ordine di pagamento e dei prestatori di servizi di informazione sui conti, il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti"*. La definizione chiarisce cosa non costituisce un dato sensibile ma non specifica, al contempo, cosa sia un dato sensibile (a parte la generica spiegazione per cui si tratta di dati che possono essere utilizzati per commettere frodi).

5 Nei casi in cui il trattamento si basa su uno specifico consenso dell'interessato, le informazioni previste dall'art. 13 sono inoltre necessarie per soddisfare il requisito del consenso "informato" (considerando 32 GDPR).

Nel caso in cui più soggetti siano coinvolti nel trattamento, come nel caso di "concorso" tra operatori bancari e TPP, si pone il **problema di stabilire chi è tenuto a fornire all'interessato l'informativa** nonché ad acquisire e conservare il relativo consenso, ove questo sia necessario.

Nella normalità dei casi, il cliente ha un primo contatto negoziale con l'operatore bancario ad esempio per l'apertura di un conto corrente o per l'emissione di una carta di pagamento.

Se in un secondo momento il cliente intende beneficiare dei servizi di un TPP, quest'ultimo sarà tenuto a fornire una nuova e diversa informativa da quella presumibilmente già presentata dalla banca?

Nel caso in cui il cliente abbia già rilasciato all'operatore bancario il consenso a che i suoi dati siano resi disponibili ad un TPP, quest'ultimo potrà avere accesso a tutti i dati del cliente conservati presso la banca, anche se non direttamente necessari per l'erogazione del servizio da esso fornito?

Si tratta solo di alcuni interrogativi che fanno emergere **l'importanza di soluzioni adeguate al caso specifico**, che concilino le diverse previsioni normative, nell'ottica di una organizzazione efficiente e conforme ad entrambe le normative.

In tale ottica sarà opportuno, nell'interesse di entrambi, operatore bancario e TPP, che siano disciplinati in via negoziale i reciproci rapporti con riferimento al trattamento dei dati personali dei clienti.

In particolare, l'inquadramento sul piano della protezione dei dati personali del TPP è uno degli aspetti che può dar luogo a maggiori criticità e controversie, a partire dalla questione se il TPP debba essere considerato titolare o responsabile del trattamento.

Ciascuna delle due ipotesi è possibile, almeno astrattamente; non sembra possibile fornire, a priori, una risposta univoca e standardizzata per tutti i TPP e i nuovi servizi PSD2; occorre infatti una valutazione, caso per caso, che tenga conto in concreto delle funzioni e delle attività svolte.

A seconda della soluzione scelta, ci saranno profili da regolare e responsabilità da ripartire: se si imponesse, nel caso concreto, di inquadrare l'operatore bancario come titolare del trattamento e il TPP come responsabile del trattamento, sarebbe necessario stipulare un contratto che, in conformità all'art. 28 del GDPR[6], disciplini il trattamento effettuato dal TPP.

In particolare l'operatore bancario, in quanto titolare del trattamento, dovrebbe fornire al TPP, in quanto responsabile del trattamento, una serie di istruzioni per la realizzazione del trattamento stesso (ad es. le misure di sicurezza da mettere in atto, eventuali tecniche di criptazione e/o pseudonimizzazione da adottare, elaborazione di procedure da seguire in caso di *data breach,* ecc.).

In aggiunta l'operatore bancario dovrà esercitare uno stretto controllo sull'operato del TPP in quanto, come titolare, è l'operatore bancario ad essere responsabile ultimo di tutte le violazioni del GDPR, anche quelle derivanti da comportamenti del responsabile del trattamento, salvo che dimostri di non essere in alcun modo responsabile.

---

6 L'art. 28(3) GDPR prevede che *"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento".*

Si pone a questo punto un primo **contrasto tra GDPR e PSD2**.

Mentre l'art. 28 del GDPR, come detto, richiede che i rapporti tra titolare e responsabile del trattamento siano disciplinati da un contratto o altro atto giuridico, gli articoli 66(5) e 67(4) della PSD2 stabiliscono che non può essere richiesto al TPP alcun contratto per accedere e usufruire dei dati personali del cliente della banca che ha scelto di avvalersi dei servizi del TPP[7]. In pratica, allo scopo di agevolare l'operatività dei TPP facilitando la diffusione dei loro servizi, il TPP ha diritto di accedere direttamente ai dati bancari (*i.e*. quelli necessari per l'erogazione del servizio del TPP) del cliente.

L'operatore bancario non può dunque rifiutarsi di concedere al TPP l'accesso ai dati del cliente che, volendo usufruire dei nuovi servizi previsti dalla PSD2, abbia deciso di avvalersi di un TTP.

Questa "discrasia" comporta che se, da un lato, l'operatore bancario è responsabile per la condotta del TPP, dall'altro lato non ha di fatto la possibilità di intervenire e limitare tale condotta.

Gli operatori bancari, già esposti agli effetti potenzialmente negativi della "**disintermediazione bancaria**", potrebbero trovarsi ben presto di fronte a un pericoloso bivio.

Nel caso in cui l'operatore bancario non riponga fiducia nelle capacità tecniche e organizzative del TPP rispetto alla *compliance privacy*, un eventuale rifiuto dell'operatore bancario di fornire i dati del cliente al TPP costituirebbe una violazione della PSD2 e, almeno astrattamente, un inadempimento nei confronti del cliente che ha deciso di avvalersi dei servizi TPP.

Viceversa, se l'operatore bancario decidesse di conformarsi alla PSD2 e fornire i dati del cliente al TPP, in caso di *data breach* e violazione delle norme a tutela della riservatezza del cliente da parte del TPP, l'operatore bancario potrebbe essere responsabile in base al GDPR (con tutto ciò che ne consegue sul profilo economico data la severità del quadro sanzionatorio previsto dal GDPR).

Altra possibilità consiste nel considerare l'operatore bancario e il TPP come due titolari autonomi del trattamento.

In tal caso si porrebbe il problema di regolare il trasferimento dei dati dall'operatore bancario al TPP.

Infatti il cliente instaura un rapporto in primo luogo con l'operatore bancario; nel momento in cui il cliente richiede al TPP l'erogazione del nuovo servizio PSD2, il TPP non raccoglie i dati direttamente dal cliente, ma li acquisisce attraverso l'accesso ai dati dell'operatore bancario.

Si configura dunque una cessione di dati dall'operatore bancario al TPP con tutto ciò che ne consegue: nel rispetto del principio di trasparenza, al cliente deve essere reso noto che i suoi dati potranno essere comunicati a un terzo (il TPP), che potrà trattarli in maniera autonoma per il perseguimento di proprie finalità. In questo caso sia l'operatore bancario che il TPP saranno soggetti all'obbligo di informare l'interessato, per quanto di propria competenza.

---

7 Le due norme richiamate nel testo stabiliscono rispettivamente che "*la prestazione di servizi di disposizione di ordine di pagamento non è subordinata all'esistenza di un rapporto contrattuale a tale scopo tra i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento di radicamento del conto*" (art. 66, comma 5, per quanto riguarda i PISP) e che, analogamente, "*la prestazione di servizi di informazione sui conti non è subordinata all'esistenza di un rapporto contrattuale a tale scopo tra i prestatori di servizi di informazione sui conti e i prestatori di servizi di pagamento di radicamento del conto*" (art. 67, comma 4, per quanto riguarda gli AISP).
Le due disposizioni normative sono state rispettivamente attuate in Italia agli articoli 5-ter e 5-quater del D.Lgs. 10/2011.

Oltre al contrasto esistente tra art. 28 del GDPR e gli artt. 66 e 67 della PSD2, si segnala un ulteriore possibile attrito applicativo: l'art. 12 del GDPR prevede che quando l'interessato esercita uno dei diritti che gli sono riconosciuti, il titolare del trattamento deve dare seguito alla richiesta entro un mese. Questa disposizione si applica anche nel caso in cui l'interessato chieda di accedere ai propri dati o di riceverli in un formato strutturato (il c.d. diritto alla portabilità dei dati).

Ai sensi della PSD2, invece, l'operatore bancario deve fornire ai TPP l'accesso ai dati in tempo reale.

In conclusione è evidente che la nuova regolamentazione in materia di protezione dei dati personali avrà un forte impatto sull'attività degli operatori bancari e dovrà essere presa in attenta considerazione nel futuro esercizio dell'attività bancaria.

Tanto agli operatori tradizionali del settore bancario, quanto ai TPP, sarà richiesto un particolare e continuo sforzo per trovare un punto di equilibrio tra le due normative (GDPR e PSD2) ed assicurare adeguata *compliance* rispetto a entrambi i fronti normativi.

Contatti

Per maggiori informazioni vi invitiamo a contattare:

Agostino Clemente
a.clemente@unlaw.it

Benedetto Colosimo
b.colosimo@unlaw.it

Ughi e Nunziante – Studio Legale