La PSD2 sotto la lente di ingrandimento del Comitato europeo per la protezione dei dati: le Linee Guida 06/2020

Silvia Capuano
Group Data Protection Regulation Specialist, Mediobanca – Banca di Credito Finanziario S.p.A.

Tommaso Sala
Head of Group Data Protection Regulation, Mediobanca – Banca di Credito Finanziario S.p.A.

1. Introduzione

Il rapporto tra il Regolamento (UE) 2016/679 ("**GDPR**" o "**Regolamento**") e la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno ("**PSD2**") sono ormai da tempo al centro di discussioni per via dei conflitti e dei dubbi interpretativi che, a livello nazionale, l'Associazione Bancaria Italiana ("**ABI**") ha portato all'attenzione del Garante per la protezione dei dati personali già all'inizio del 2018. In quell'occasione, l'allora Presidente dell'Autorità, Antonello Soro, condividendo le criticità evidenziate dall'ABI, aveva predisposto una nota indirizzata al Consiglio dei ministri, auspicando che la normativa adottata in attuazione del decreto legislativo di recepimento della PSD2[1] potesse costituire il momento propizio per definire un quadro normativo chiaro e condiviso in relazione ai profili di protezione dei dati

[1] Decreto Legislativo 15 dicembre 2017, n. 218, Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

personali sottesi alla disciplina[2]. Anche a livello europeo, la relazione tra le due normative è stata oggetto di alcuni interventi: da parte della European Banking Authority ("**EBA**"), nell'ambito delle risposte ai quesiti che le sono stati sottoposti dagli stakeholder[3], sull'applicazione pratica della PSD2; e da parte del Comitato europeo per la protezione dei dati ("**Comitato**" o "**EDPB**")[4], con la risposta alla lettera dell'europarlamentare Sophie in't Veld, in cui sono state fornite le prime indicazioni su alcuni punti controversi e, in particolare, sul trattamento dei dati delle c.d. "*silent parties*"[5], nonché sul concetto di consenso esplicito di cui all'articolo 94 della PSD2[6].

L'attenzione dell'EDPB non si è tuttavia esaurita con tale intervento: l'interazione tra GDPR e PSD2 è stata infatti una delle questioni che ha maggiormente impegnato il sottogruppo di esperti "*Financial Matters*" – trattandosi di normative chiave della legislazione europea degli ultimi anni[7] – ed è sfociata nell'adozione delle Linee Guida 06/2020[8] ("**Linee Guida**"), avvenuta in data 15 dicembre 2020, a seguito di una vivace consultazione pubblica, grazie ai numerosi *feedback* trasmessi dagli *stakeholder* tra luglio e settembre 2020[9].

La necessità di un autorevole intervento trova origine dall'impianto stesso della PSD2 che, relativamente alla protezione dei dati degli utenti, detta regole piuttosto austere che, nella sostanza, si limitano a vietarne un uso diverso da quello direttamente correlato all'attività tipica dei Third Party Providers[10], come definiti successivamente, lasciando aperti numerosi interrogativi, ricchi di riflessi anche sul piano pratico e applicativo[11].

[2] Nota del Presidente del Garante, Antonello Soro, al Presidente del Consiglio dei ministri in tema di direttiva sui servizi di pagamento (cd. PSD2) del 9 gennaio 2018, disponibile al sito: http://bit.ly/32xr54a.

[3] Cfr. C. Bernasconi, E. M. Scavoni, T. Sala, F. Messina, *Il GDPR nell'operatività dei Third Party Providers (TPPs)*, in *Privacy&, n. 4 febbraio 2020*, p. 91.

[4] Il Comitato europeo per la protezione dei dati è un organo europeo indipendente, composto dai rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. Tra i compiti attribuitigli dall'articolo 70 del GDPR, vi è quello di contribuire all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea che avviene, inter alia, con la pubblicazione di linee guida.

[5] Per "*silent parties*" si intendono i beneficiari dei pagamenti.

[6] Lettera di risposta a Sophie in't Veld da parte del Comitato europeo per la protezione dei dati, disponibile sul sito: http://bit.ly/3gtKD1x.

[7] Relazione 2019 del Garante per la protezione dei dati personali, p. 193.

[8] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, disponibili sul sito: http://bit.ly/32FHeEJ.

[9] I *feedback* degli *stakeholder* sono consultabili sul sito: http://bit.ly/2RS2ViZ.

[10] Cfr. Francesco Ciraolo, *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*, in *Rivista di Diritto Bancario* – Dottrina e giurisprudenza commentata, Ottobre/Dicembre 2020, pp. 611-650.

[11] Cfr. M. Rabitti, A. Sciarrone Alibrandi, *I servizi di pagamento tra PSD2 e GDPR: open*

A dispetto dell'indubbia rilevanza del problema, basti pensare, *inter alia*, al differente significato che le due normative assegnano al concetto di "dati sensibili"[12] e "consenso"[13], sovrapponibili solo da un punto di vista terminologico; oppure alle incertezze in tema di trattamento dei dati delle c.d. "*silent parties*"[14], i cui dati personali possono essere trattati in assenza di consenso; o, ancora, ai criteri per individuare chi, tra il fornitore di servizi di pagamento, c.d. *Account Servicing Payment Service Provider*[15] ("**ASPSP**") – tipicamente la banca – e i nuovi operatori del mercato, i c.d. Third Party Providers ("**TPPs**") – il prestatore di servizi di disposizione di ordine di pagamento o il prestatore di servizi di informazione sui conti – rivestano il ruolo di titolare del trattamento o responsabile del trattamento[16], con evidenti conseguenze in termine di responsabilità.

Muovendo da tali dubbi interpretativi e considerate le preoccupazioni sull'effettivo controllo dei dati personali da parte dei correntisti, in un contesto in cui, almeno potenzialmente, l'open banking apre alle *FinTech Companies* la possibilità di acquisire notevoli quantità di dati relativi ai conti di pagamento, le Linee Guida non si limitano a fornire ulteriori indicazioni sul rapporto tra le disposizioni del GDPR e della PSD2, ma chiariscono la

banking e conseguenze per la clientela, in F. Capriglione, *Liber amicorum* Guido Alpa, Cedam, 2019, pp. 726-727.

[12] Per la PSD2, intesi genericamente come i dati relativi ai pagamenti che possono essere utilizzati per commettere frodi, mentre per il GDPR sono quelli concernenti l'origine razziale o etnica, le opinioni politiche o le convinzioni religiose, l'appartenenza sindacali, la salute, i dati genetici o biometrici, la vita o l'orientamento sessuale.

[13] Per la PSD2 il consenso relativo all'accesso, alla trattazione e conservazione dei dati personali è di tipo contrattuale e relativo alla prestazione dei servizi di pagamento, mentre per il GDPR il consenso è una condizione di liceità di portata più generale, applicabile ai soli trattamenti di dati che lo richiedono (es. per i dati relativi alla salute o nei trattamenti per finalità di marketing).

[14] Cfr. nota 5.

[15] Letteralmente "Prestatore di servizio di pagamento di radicamento del conto", che è il soggetto vigilato presso cui l'utente detiene il conto di pagamento; cfr. articolo 4, punto 17, PSD2, "'prestatore di servizi di pagamento di radicamento del conto': un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore".

[16] Per alcuni, "*when a bank receives data from another bank or institution and is processing the data under its own terms, then the bank is a processor. So, in this regard, if data moves from the bank to a TPP, the bank is the controller and the TPP (AISP or PISP) is a processor instructed by the data controller*". Cfr. Helgadottir, Dilja, The Interaction Between Directive 2015/2366 (EU) on Payment Services (PSD2) and Regulation (EU) 2016/679 on General Data Protection (GDPR) Concerning Third Party Players (December 12, 2019), in SSRN: bit.ly/3ei2Nkp). Per altri, laddove manchi un rapporto contrattuale tra ASPSP e TPP che stabilisca chi fra i soggetti coinvolti sia il titolare e chi il responsabile del trattamento, entrambi i soggetti potrebbero essere ritenuti titolari del trattamento. Cfr. M. Rabitti, A. Sciarrone Alibrandi, *cit*., p. 730-731; Cfr. European Banking Federation, *Guidance for implementation of the revised Payment Services Directive*, Dicembre 2019, 84.

reale estensione, i requisiti e le garanzie del trattamento di tali dati personali da parte dei TPPs.

2. La PSD2 in pillole

La PSD2 può definirsi figlia della Direttiva 2007/64/CE ("**Payment Services Directive 1**" o "**PSD1**")[17], che ha introdotto una disciplina unitaria[18] dei servizi di pagamento. Tuttavia, a poca distanza dalla sua emanazione, il progressivo sviluppo tecnologico e i rapidi cambiamenti hanno avuto un impatto di straordinaria rilevanza sul sistema finanziario[19], tanto da rendere necessario un nuovo intervento da parte del legislatore comunitario, anche al fine di regolamentare alcuni servizi di pagamento innovativi che non venivano in tutto o in parte disciplinati dalla PSD1[20].
Ebbene, nel 2015 il legislatore comunitario ha quindi adottato la PSD2, recepita in Italia tramite il D.Lgs. 15 dicembre 2017, n. 218, che ha modificato il D.Lgs. 27 gennaio 2010, n. 11, e il capo II bis del Titolo VI del TUB.

[17] La PSD1 è stata recepita in Italia attraverso il Decreto Legislativo 27 gennaio 2010, n. 11, il quale ha introdotto il capo II bis del Titolo VI del Decreto Legislativo 1 settembre 1993, n. 385 (TUB).

[18] Cfr. O. Troiano, *La disciplina uniforme dei servizi di pagamento: aspetti critici e proposte ricostruttive,* in M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, (a cura di), *Armonizzazione europea dei servizi di pagamento e attuazione della Direttiva 2007/64/CE*, Milano, 2009, p. 15, "*l'innegabile esigenze di regole europee non comportava pure che si ponesse mano ad una disciplina unitaria di tutti i servizi di pagamento. Questa scelta ulteriore – non necessaria ai fini del mercato interno – è stata fatta dal legislatore quasi in sordina, ma rappresenta un punto qualificante della Direttiva e, soprattutto, il punto di rottura rispetto alla tradizione delle discipline nazionali*"

[19] Cfr. F. Cascinelli, V. Pistoni, G. Zanetti, *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in *Diritto Bancario*, 2016.

[20] Cfr. F. Cascinelli, V. Pistoni, G. Zanetti, *cit.*; cfr. considerando (27) PSD2, "*Successivamente all'adozione della direttiva 2007/64/CE si sono diffusi nuovi tipi di servizi di pagamento, specialmente nel settore dei pagamenti tramite Internet. In particolare, si sono evoluti i servizi di disposizione di ordine di pagamento nel settore del commercio elettronico. Tali servizi di pagamento svolgono un ruolo nei pagamenti in detto settore mediante un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici*"; cfr. inoltre Commissione europea, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 2002/65/CE, 2013/36/UE e 2009/110/CE e che abroga la direttiva 2007/64/CE", COM(2013) 547, 2013, p. 2, "Insieme alla crescita costante del numero di pagamenti con carta di credito e con carta di debito, l'affermarsi del commercio elettronico e la popolarità sempre maggiore degli smartphone hanno spianato la strada alla diffusione di nuovi mezzi di pagamento […] soprattutto pagamenti effettuati con carte e nuovi mezzi di pagamento, come internet e dispositivo mobile, sono spesso ancora frammentati lungo i confini nazionali così che diventa difficile sviluppare efficacemente servizi di pagamento digitali innovativi e di facile utilizzo"; cfr. inoltre C. Bernasconi, E. M. Scavoni, T. Sala, F. Messina, *cit*.

La nuova normativa, pur mantenendo l'impostazione generale della PSD1, è intervenuta per disciplinare le attività svolte dai TPPs, che si suddividono in:

- "Payment Initiation Service Provider" (c.d. "PISP"), letteralmente il "Prestatore di servizi di disposizione di ordine di pagamento", che fornisce servizi per avviare ordini di pagamento, su richiesta di un utente – persona fisica o giuridica – con addebito su un conto di pagamento[21] detenuto presso un ASPSP, tipicamente una banca;
- "*Account Information Service Provider*" (c.d. "AISP"), letteralmente il "Prestatore di servizi di informazione sui conti", che fornisce servizi online relativamente a informazioni consolidate su uno o più conti di pagamento detenuti dall'utente – persona fisica o giuridica – presso uno o più prestatori di servizi di pagamento.

In buona sostanza, il servizio di disposizione di ordini di pagamento presuppone che il PISP si frapponga tra il pagatore e il suo conto di pagamento online, dando impulso all'operazione a favore di un beneficiario[22], sostituendosi all'utente nell'invio dell'ordine di pagamento alla ASPSP. In tal modo si verifica un'agevolazione nel rapporto con il beneficiario, rendendo possibile informare quest'ultimo in via immediata dell'avvio dell'ordine, velocizzando la spedizione e/o l'accesso ai beni e servizi acquistati online[23].
Il servizio di informazione sui conti (AISP), invece, consiste nella raccolta,

[21] Cfr. Ai sensi dell'articolo 4, punto 12, PSD2, "un conto detenuto a nome di uno o più utilizzatori di servizi di pagamento utilizzato per l'esecuzione di operazioni di pagamento"; cfr. Corte di Giustizia UE, C-191/17, § 30-31, "Al riguardo, occorre prendere in considerazione l'articolo 1, paragrafo 6, della direttiva sui conti di pagamento, che prevede che quest'ultima si applichi ai conti di pagamento che consentono ai consumatori di effettuare quanto meno le operazioni che consistono nel versamento di fondi su un conto di pagamento, nei prelievi in contante su un conto di pagamento e nell'eseguire e ricevere operazioni di pagamento, compresi i bonifici, a favore di terzi e da questi ultimi. Ne deriva che la possibilità di effettuare a partire da un conto operazioni di pagamento a favore di terzi e da questi ultimi rappresenta un elemento costitutivo della nozione di "conto di pagamento".

[22] Cfr. F. Cascinelli, V. Pistoni, G. Zanetti, *cit*.

[23] Cfr. Commissione Europea, Payment Services Directive: frequently asked questions, Bruxelles, 2018, Question 18, in cui si afferma inoltre "For online payments, they constitute a true alternative to credit card payments as they offer an easily accessible payment service, as the consumer only needs to possess an online payment account"; cfr. S. Vanini, *cit.*, "Il principale vantaggio che deriva all'utente dall'avvalersi del servizio in analisi va apprezzato in termini di accountability: l'esercente-beneficiario, infatti, ricevendo conferma dal PISP circa l'effettiva disposizione dell'ordine, sarà incentivato ad eseguire la prestazione a suo carico (ad es., consegna della merce, erogazione del servizio) senza alcuna esitazione. A ciò si aggiungono ulteriori servizi accessori che generalmente i prestatori di servizi di disposizione di ordine di pagamento offrono agli utenti per l'incremento della soglia di sicurezza dell'operazione o che derivano dalle promozioni di fidelizzazione".

aggregazione e messa a disposizione dell'utente di informazioni online su uno o più conti di pagamento detenuti presso un altro o altri soggetti, a cui si ha accesso mediante interfacce online. Gli utenti, pertanto, possono avere una visione globale della loro situazione finanziaria, ottenuta attraverso informazioni consolidate relative a più conti di pagamento, agevolando la pianificazione finanziaria mediante, per esempio, la classificazione delle spese in base alle diverse tipologie di beni/servizi[24].

Ebbene, entrambi i servizi, prevedendo un rilevante scambio di dati dei conti di pagamento intrattenuti dagli utenti presso banche o altri enti autorizzati, comportano implicazioni tutt'altro che secondarie in materia di protezione dei dati personali e, in particolare, sui diritti e le libertà degli utenti[25], nonché in termini di rischi per la sicurezza e la riservatezza delle informazioni.

3. I ruoli privacy dei "payment service providers"

Uno degli aspetti che la versione in consultazione pubblica delle Linee Guida non metteva in luce era l'aspetto relativo ai criteri per individuare i "ruoli privacy" delle parti coinvolte nei servizi disciplinati dalla PSD2.

Come noto, l'obbligo degli ASPSPs di consentire l'accesso ai TPPs, anche in assenza di un rapporto contrattuale con questi ultimi, lasciava aperti numerosi interrogativi circa le conseguenze da un punto di vista privacy, poiché il GDPR impone una chiara identificazione dei ruoli delle parti che a vario titolo intervengono nel trattamento.

A tal proposito, il Regolamento individua due principali figure: il titolare del trattamento, ovvero colui che determina finalità e i mezzi del trattamento di dati personali e il responsabile del trattamento, che tratta i dati per conto del titolare.

Sul punto, richiamando le Linee guida 07/2020 sul concetto di titolare e responsabile del trattamento[26], che rappresentano una bussola per orientare scelte coscienti e coerenti da parte degli operatori rispetto alle disposizioni del GDPR, il Comitato, con le Linee Guida, ha adottato un approccio conservativo – in piena coerenza con il principio di *accountability* – affermando, nella sostanza, che i ruoli ricoperti dai TPPs non possono essere stabiliti a priori, ma dovranno essere valutati di volta in volta dalle parti, tenendo conto delle circostanze del caso.

[24] Cfr. Commissione europea, Payment Services Directive: frequently asked questions, Bruxelles, 2018, Question 19.

[25] Cfr. F. Marasà, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, in *Orizzonti del Diritto Commerciale*, Fascicolo 2/2020.

[26] Cfr. http://bit.ly/3nbkciz.

Tale approccio è pienamente condivisibile, se si considera che il principio di *accountability* ha sancito in modo ufficiale e definitivo il passaggio da un approccio formale, che si traduceva nell'adozione da parte dei titolari e responsabili del trattamento delle misure minime già individuate dalle autorità di controllo, a un approccio sostanziale, in cui le autorità di controllo, Comitato incluso, devono limitarsi a fornire ausili interpretativi e analitici, demandando ai titolari e responsabili del trattamento il compito e le responsabilità di decidere in autonomia modalità e limiti del trattamento dei dati personali, ciò nondimeno nell'ambito dell'individuazione dei ruoli privacy dei TPPs.

In questa logica, spetterà a PISP e AISP valutare, in primo luogo, a seconda delle circostanze specifiche del trattamento e nel pieno rispetto del principio di *accountability*, quale veste ricoprono nel trattamento dei dati degli utenti, formalizzando, in seconda istanza, gli eventuali adempimenti richiesti dalla normativa (es. la nomina a responsabile del trattamento) ancor prima di avviare il trattamento, secondo un approccio di *privacy by design*.

Ciò che invece sembrerebbe essere fuori discussione, è il ruolo di titolari del trattamento degli ASPSPs che, come vedremo, si devono limitare a concedere l'accesso ai conti di pagamento ai TPPs.

4. La principale base giuridica per il trattamento dei dati da parte di PISP e AISP e l'accesso ai conti di pagamento degli utenti presso gli ASPSPs

La PSD2, in diverse occasioni, richiama espressamente la normativa privacy[27], riportando alcuni dei principi fondamentali applicabili al trattamento dei

[27] Cfr. Considerando (89): "*La prestazione di servizi di pagamento da parte dei prestatori di servizi di pagamento può comportare il trattamento di dati personali. La direttiva 95/46/CE del Parlamento europeo e del Consiglio, le norme nazionali che danno attuazione alla direttiva 95/46/CE e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio si applicano al trattamento dei dati personali ai fini della presente direttiva. In particolare, qualora ai fini della presente direttiva vi sia trattamento di dati personali, è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui alla direttiva 95/46/CE e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre, la protezione dei dati fin dalla progettazione e la protezione dei dati di default dovrebbero essere integrate in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nel quadro della presente direttiva*"; Considerando (90): "*La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, incluso il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali, la libertà d'impresa, il diritto a un ricorso effettivo e il diritto di non essere giudicati o puniti due volte per lo stesso reato. La presente direttiva deve essere applicata conformemente a tali diritti e principi*".

dati personali. Un chiaro riferimento al GDPR si rinviene nell'articolo 94[28] che sancisce il consenso prestato dall'utente[29] come esclusiva base giuridica legittima affinché i TPPs possano trattare e conservare i dati personali necessari alla prestazione dei rispettivi servizi, informando l'utente persona fisica del servizio[30], in conformità con la Direttiva 95/46/CE[31], relativamente al trattamento dei suoi dati personali.

A tal proposito, le Linee Guida avvalorano quanto già affermato dal Comitato con la lettera adottata in data 5 luglio 2018, in risposta alla deputata del Parlamento europeo Sophie In't Veld.

In particolare, viene ribadito, *semel pro semper*, che il consenso esplicito di cui all'articolo 94 della PSD2 ha natura contrattuale, non assimilabile alla manifestazione di volontà dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a) del GDPR in quanto, sebbene correlato ai dati personali e alla loro protezione, rappresenta l'espressione della volontà dell'utente che consente ai TPPs di ottenere l'accesso ai suoi dati personali, allo scopo di fornire il servizio.

Analogamente a quanto affermato in tema di individuazione dei ruoli privacy, le Linee Guida prevedono, in linea generale, che spetta ai titolari del trattamento definire la base giuridica appropriata, che dipende dalle caratteristiche del trattamento, ivi incluse finalità e relazione tra il titolare del trattamento e l'interessato.

[28] "*1. Gli Stati membri autorizzano il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. La fornitura di informazione a persone fisiche in merito al trattamento dei dati personali e al trattamento di tali dati personali e di qualsiasi altro trattamento di dati personali ai fini della presente direttiva è effettuata in conformità della direttiva 95/46/CE, delle norme nazionali di recepimento della direttiva 95/46/CE e del regolamento (CE) n. 45/2001. 2. I prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo dietro consenso esplicito dell'utente dei servizi di pagamento*".

[29] L'ambito di applicazione delle due discipline rappresenta un ulteriore elemento di differenza: infatti, mentre il GDPR è volto alla tutela delle persone fisiche, la PSD2 mira alla protezione degli utenti di servizi di pagamento in generale. In tal senso cfr. A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services Questioni regolamentari e profili di business*, in *CONSOB*, Quaderni Fintech N. 4, Marzo 2019, pp. 33 e ss. Disponibile al sito: http://bit.ly/3v8LskB.

[30] L'ambito di applicazione delle due discipline rappresenta un ulteriore elemento di differenza: infatti, mentre il GDPR è volto alla tutela delle persone fisiche, la PSD2 mira alla protezione degli utenti di servizi di pagamento in generale. In tal senso cfr. A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services Questioni regolamentari e profili di business*, in *CONSOB*, Quaderni Fintech n. 4, Marzo 2019, pp. 33 e ss. Disponibile al sito: http://bit.ly/3v8LskB.

[31] All'epoca dell'entrata in vigore della PSD2, il GDPR era ancora in fase di approvazione.

Tuttavia, dalla lettura del Considerando (87) della PSD2[32], si evince che i servizi di pagamento sono forniti sulla base di un contratto tra l'utente e il prestatore di tali servizi.
Il Comitato ha pertanto ritenuto che l'idonea base giuridica del trattamento dei dati da parte di PISP e AISP sia rappresentata dall'esecuzione del contratto di cui l'interessato (*rectius* l'utente) è parte o di misure precontrattuali adottate su richiesta dello stesso, ai sensi dell'articolo 6, paragrafo 1, lett. b), GDPR, fermo restando l'obbligo da parte dei TPPs di ottenere il "consenso contrattuale" dall'utente e dimostrare che senza il conferimento dei dati da parte dell'interessato, il contratto o le misure precontrattuali non sarebbero eseguibili.
Ebbene, può affermarsi che l'esercizio delle attività dei TPP postula necessariamente il "consenso contrattuale" dell'utente, sussistendo il quale il fornitore terzo è autorizzato ad accedere ai conti accesi presso un ASPSP, indipendentemente dalla stipula di un accordo "negoziale" con quest'ultimo.
In virtù di un "consenso contrattuale" dell'utente, l'ASPSP concede ai TPPs l'accesso al conto al fine di consentire all'utente di avvalersi dei servizi disciplinati dalla PSD2.
L'EDPB ha pertanto trovato campo fertile nell'individuazione della condizione di liceità che consente agli ASPSPs di concedere ai TPPs l'accesso ai conti di pagamento degli utenti – ivi inclusi ai loro dati personali – atteso che esso rappresenta l'adempimento di un obbligo legale a cui gli ASPSPs stessi sono sottoposti.
Tale accesso è infatti la condizione necessaria affinché i TPPs possano fornire i loro servizi e garantire i diritti previsti dagli articoli 66, paragrafo 1, e 67, paragrafo 1, della PSD2, indipendentemente da qualsivoglia "consenso privacy".

5. Il trattamento dei dati personali degli utenti per finalità ulteriori

Le Linee Guida contemplano altresì la fattispecie in cui il trattamento dei dati personali degli utenti sia necessario nell'ambito della prestazione da parte dei TPPs di diversi e separati servizi o loro elementi che possono essere ragionevolmente eseguiti indipendentemente l'uno dall'altro.
Nella fattispecie, i TPPs sono chiamati a dimostrare l'indefettibile rapporto causale intercorrente tra il conferimento di dati personali e l'esecuzione di

[32] "*La presente direttiva dovrebbe riguardare solo gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento*".

ciascuno di tali servizi, in assenza del quale non si potranno appellare all'articolo 6, paragrafo 1, lettera b) del GDPR e saranno costretti a considerare una base giuridica differente dall'esecuzione del contratto di cui l'utente è parte o di misure precontrattuali da adottare su richiesta dello stesso.
A tal proposito, il tenore letterale degli articoli 66 e 67 della PSD2 sembra precludere la strada a ulteriori trattamenti.
Invero, l'articolo 66, paragrafo 2, lett. g), della PSD2, relativamente ai PISP, prevede che essi non usino né conservino dati né vi accedano "*per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento come esplicitamente richiesto dal pagatore*". Al contempo, l'articolo 67, paragrafo 2, lett. f), della PSD2, relativamente agli AISP, prevede che essi non usino, accedano o conservino dati "*per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati*".
Tuttavia, la normativa in materia di protezione dei dati personali non vieta a priori al titolare di trattare i dati anche per finalità ulteriori rispetto a quelle oggetto del contratto o della richiesta specifica dell'interessato, purché il trattamento sia supportato da una legittima base giuridica quale, ad esempio, il consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), del GDPR, e sia preceduto da una completa informativa.
Sul punto, le Linee Guida, richiamando l'articolo 6, paragrafo 4, del GDPR[33], concludono che, sebbene le disposizioni della PSD2 non consentano ai TPPs di trattare i dati per altre finalità, sul piano giuridico tale ulteriore trattamento è consentito in presenza di un consenso dell'interessato o della necessità di adempiere a un obbligo legale previsto dal diritto dell'Unione o dello Stato membro al quale è soggetto il titolare.
Tra i trattamenti dei dati personali degli utenti da parte dei TPPs per "*finalità connesse a un atto legislativo dell'Unione o di uno Stato membro*", il Comitato

[33] Cfr. Articolo 6, paragrafo 2 del GDPR: "*Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: (C50) a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*".

annovera la prevenzione e il contrasto delle frodi, come peraltro previsto dall'articolo 94, paragrafo 1, della PSD2[34] che, secondo le Linee Guida in esame, può altresì basarsi sul legittimo interesse dei PISP e degli AISP, ai sensi dell'articolo 6, paragrafo 1, lettera f), del GDPR, "[…] *a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*".
Resta fermo il divieto generale per i TPPs di utilizzare, nel proprio interesse e per proprio conto, i dati personali degli utenti per finalità differenti rispetto a quelle per le quale gli stessi sono stati raccolti, in conformità al generale principio della limitazione delle finalità del trattamento, di cui all'articolo 5, paragrafo 1, lett. b), del GDPR.

6. Il trattamento dei dati delle c.d. "*silent parties*"

Ulteriore ventaglio di problematiche suscita il trattamento dei dati delle parti silenti ovvero dei beneficiari dei pagamenti.
Più in dettaglio, l'esecuzione del contratto tra gli utenti e i TPPs comporta un accesso ai conti di pagamento degli utenti e, di conseguenza, anche ai dati di coloro che, relativamente a quel determinato conto di pagamento, hanno effettuato delle operazioni; basti pensare ai dati del beneficiario di un bonifico o di colui che lo dispone.
Significativa appare, dunque, l'individuazione di un'idonea base giuridica per il trattamento dei dati personali delle c.d. "silent parties" da parte dei TPPs.
Sul punto, l'EDPB non si discosta rispetto a quanto aveva in precedenza affermato[35] chiarendo che il legittimo interesse del titolare del trattamento o di un terzo costituisce una valida base giuridica per il trattamento dei dati della parte silente, purché vengano rispettati i principi di minimizzazione, limitazione e trasparenza – anche mediante l'utilizzo di misure di sicurezza quali la cifratura – e i dati vengano utilizzati solo ai fini dell'erogazione del servizio richiesto dall'utente.
Al fine di sgomberare il campo da ogni dubbio, il Comitato precisa che, salvo

[34] Cfr. Articolo 94, paragrafo 1, della PSD2 "*Gli Stati membri autorizzano il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. La fornitura di informazione a persone fisiche in merito al trattamento dei dati personali e al trattamento di tali dati personali e di qualsiasi altro trattamento di dati personali ai fini della presente direttiva è effettuata in conformità della direttiva 95/46/CE, delle norme nazionali di recepimento della direttiva 95/46/CE e del regolamento (CE) n. 45/2001*".
[35] Il riferimento è alla lettera indirizzata al Parlamento europeo in data 5 luglio 2018 già citata in precedenza.

i casi previsti dal diritto dell'Unione o degli Stati membri, è escluso qualsiasi trattamento non riconducibile all'esecuzione del contratto tra TPPs e utente, non potendo trovare applicazione altra base giuridica.
D'altronde, non vi è dubbio che il contesto in cui i dati personali delle parti silenti vengono trattati, caratterizzato dall'assenza di un qualsivoglia collegamento negoziale tra gli stessi e i TPPs, non rappresenti un terreno fertile per trattamenti basati sul consenso – giuridicamente non percorribili – o per quelli che le parti silenti non possono ragionevolmente aspettarsi, ad esempio il *direct marketing*.

7. Il trattamento dei "dati sensibili" ai sensi della PSD2

Abbiamo già avuto modo di evidenziare che la definizione di "dati sensibili" ai sensi della PSD2, trova riscontro nel GDPR ma in termini differenti[36].
Invero, per la normativa privacy, i c.d. "dati sensibili" – oggi definiti dall'articolo 9, GDPR, quali categorie particolari di dati personali – sono quelli idonei a rivelare "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".
Diversamente, i dati sensibili relativi ai pagamenti di cui all'articolo 4, n. 32, della PSD2 sono quelli che "*possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate. 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*".
Le Linee Guida, sebbene confermino la profonda diversità dei due concetti, si limitano a raccomandare ai TPPs di mappare e categorizzare con precisione il tipo di dati personali oggetto di trattamento, in funzione della definizione data dalle due discipline, anche ai fini dell'effettuazione di una valutazione d'impatto ai sensi dell'articolo 35 del GDPR che, per la tipologia di rischi per i diritti e le libertà degli interessati connessi a tali servizi, non sembrerebbe essere evitabile.
Il Comitato focalizza i propri sforzi su una questione ben più complicata, ovvero l'individuazione dell'idonea base giuridica per il trattamento delle categorie particolari di dati personali da parte dei TPPs.
Con il significativo incremento dei pagamenti elettronici, è quantomai

[36] La medesima discrepanza è rilevabile anche in quanto previsto dagli articoli 5-ter, c. 2, lett. e), e 5-quater, c. 2, lett. e), d.lgs. 11/2010, che hanno attuato in Italia le disposizioni in esame.

improbabile che le transazioni che vengono effettuare quotidianamente non contengano categorie particolari di dati, basti pensare ai dati relativi alla salute che si possono evincere dalle fatture mediche pagate dall'interessato al proprio medico.
Ne consegue che un trattamento di tali categorie di dati da parte dei TPPs, potrà essere lecito solo in presenza di una delle deroghe previste dall'articolo 9, paragrafo 2, del GDPR che, tuttavia, mal si conciliano con il contesto in cui tale trattamento viene svolto.
Sul punto le Linee Guida sono perentorie: le uniche basi giuridiche applicabili al trattamento delle categorie particolari di dati nell'ambito della PSD2 sono rappresentate dal consenso dell'interessato o dal motivo di interesse pubblico, rispettivamente ai sensi delle lettere a) e g) dell'articolo 9, paragrafo 2, del GDPR.
Seppur concettualmente condivisibile, sul piano pratico, tale interpretazione potrebbe creare non pochi problemi ai TPPs.
Da un lato, infatti, se invocati, i motivi di interesse pubblico rilevante ai sensi dell'articolo 9, paragrafo 2, lettera g), GDPR, dovranno essere accompagnati dalle stringenti condizioni richieste dalla norma per potervi ricorrere e, in particolare, proporzionalità, rispetto dell'essenza del diritto alla protezione dei dati e previsione di idonee misure tecniche e organizzative per tutelare i diritti fondamentali e gli interessi degli interessati.
Dall'altro lato, ove non trovasse spazio tale base giuridica, i TPPs si vedrebbero costretti, in via residuale, a raccogliere il consenso dell'interessato, nel rispetto di quanto previsto dall'articolo 7 del GDPR e delle Linee guida 05/2020 dell'EDPB. Qualora anche tale deroga non fosse applicabile e ove il consenso venisse negato, i TPPs dovranno approntare idonee misure tecniche per impedire il trattamento di tali categorie particolari di dati.

8. Conclusioni

Per concludere, la coesistenza dei due dettati normativi non era apparsa, fin da subito, affatto semplice, destando più di qualche preoccupazione per la protezione dei dati personali che, giocoforza, necessitava di un autorevole pronuncia, trattandosi di disposizioni preordinate, peraltro, al raggiungimento di finalità non del tutto coincidenti.
Da un lato, il GDPR, determinante per il superamento della frammentazione normativa che ha caratterizzato il panorama europeo negli ultimi decenni, ha creato una disciplina omogenea orientata alla tutela del diritto di ogni persona fisica alla protezione dei propri dati personali. Dall'altro lato, la PSD2 e, più in generale, le norme sull'open banking, non muovendo da tali

principi, appaiono maggiormente concentrate sulla necessità di garantire un'apertura concorrenziale del mercato dei servizi di pagamento a nuovi intermediari (PISP e AISP), obiettivo che presuppone, tuttavia, la contestuale tutela dei dati dei titolari dei correntisti (non necessariamente persone fisiche), compatibilmente con la disciplina di carattere generale.
Le Linee Guida segnano, quindi, un passaggio fondamentale nell'efficace coordinamento delle disposizioni della PSD2 e del GDPR e un importante traguardo nel generale lavoro di contribuzione alla coerente applicazione delle norme sulla protezione dei dati iniziato dal Working Party Article 29.