Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR

The processing of personal data of payment service users between PSD2 and GDPR

Flaminia Marasà *

ABSTRACT:

Il lavoro verte sull'interferenza tra la disciplina del Regolamento (Ue) 679/2016 sul trattamento dei dati personali delle persone fisiche (GDPR) e quella della Direttiva (Ue) 2015/2366 sui servizi di pagamento elettronici (PSD2) per ciò che riguarda il trattamento dei dati personali dell'utente. In particolare, l'attenzione si focalizza sul ruolo svolto dagli intermediari bancari (PSP) e dai nuovi prestatori dei servizi di pagamento (*Third Party Provider*), sui limiti loro posti da entrambe le normative al trattamento dei dati degli utenti dei servizi di pagamento e sulla verifica se dal combinato disposto di tali normative consegua effettivamente una loro maggior tutela.

Parole chiave: servizi di pagamento – dati personali dell'utente – *Third Party Provider*

This article focuses on the overlapping between Regulation no. 679/2016 on the processing of personal data of natural persons (GDPR) and Directive no. 2015/2366/EU on electronic payment services (PSD) with reference to users' personal data processing. Special attention is devoted to the role played by PSP banks and new payment service providers (Third Party Providers), and to the restrictions imposed on these intermediaries by both GDPR and PSD2 in processing personal data of payment service users. The aim is to determine whether the combined provisions of these regulations achieve a more effective protection for payment service users.

***Keywords**: payment services – payment service users' personal data – Third party Provider*

SOMMARIO:

* Dottoressa di ricerca in Business, Institution and markets. E-mail: flaminia.m25@gmail.com.

servizi di pagamento e GDPR. – 5. *Segue*: il ruolo del PSP di radicamento del conto e dei TPP nel trattamento dei dati personali. – 6. Utilizzo e limiti al trattamento dei dati personali da parte degli intermediari. – 7. Il trattamento dei dati personali del beneficiario.

1. *Premesse.*

Negli ultimi anni, il continuo progresso della tecnologia ha portato alla diffusione dell'*e-commerce*, cambiando le abitudini dei consumatori e degli imprenditori e inducendoli anche all'utilizzo di nuove modalità di pagamento. Da qui il rapido affermarsi dei servizi di pagamento elettronici che ha suggerito al legislatore comunitario di elaborare un quadro normativo in grado di conciliare l'esigenza di servizi di pagamento rapidi ed efficienti con la necessità di garantire la sicurezza degli stessi.

Com'è noto, il primo testo normativo unitario, teso a disciplinare in maniera uniforme le diverse attività riferibili ad un'operazione di pagamento – intesa come «l'atto disposto dal pagatore o per suo conto o dal beneficiario, di collocare, trasferire o ritirare fondi, indipendentemente da eventuali obblighi sottostanti tra il pagatore e il beneficiario» (art. 4, par. 1, n. 5, PSD) - è stato la Direttiva (Ce) 2007/64, (*Payment Service Directive – PSD*) [1], attuata in Italia con il d.lgs. n. 11/2010. Tuttavia, a pochi anni di distanza dalla sua emanazione, le nuove opportunità offerte dall'innovazione tecnologica e i rischi ad esse connessi, hanno reso necessario, nel 2015, un nuovo intervento sul tema da parte del legislatore comunitario [2].

La PSD2 [Direttiva (Ue) 2015/2366] [3], recepita in Italia con il d.lgs. n.

[1] Gli obiettivi dichiarati della PSD (elaborati per rafforzare la SEPA, ovvero la *Single European Payment Area*) erano quelli di: sostenere la creazione di un mercato unico dei servizi di pagamento delineando un quadro giuridico di riferimento unitario; aumentare la concorrenza tra gli operatori dei mercati nazionali dei pagamenti, anche permettendo l'accesso al mercato a nuove figure di operatori economici a parità di condizioni con gli intermediari bancari; accrescere la trasparenza, introducendo uno specifico gruppo di norme per regolare le informazioni da fornire agli utenti; uniformare gli obblighi e i diritti previsti dalle singole legislazioni sia per gli utenti che per i prestatori di servizi.

[2] Il Considerando n. 3 della PSD2 sottolinea che «*la rapida crescita dei pagamenti elettronici e tramite dispositivo mobile e con la commercializzazione di nuovi tipi di servizi di pagamento, il mercato dei pagamenti al dettaglio ha registrato considerevoli innovazioni tecniche che rimettono in discussione il quadro attuale*».

[3] Sulle novità della PSD2, in generale, v. F. CASCINELLI, *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, reperibile in internet al seguente indirizzo:

218/2017[4], pur mantenendo l'impostazione generale della precedente Direttiva[5], ha posto l'attenzione sulla regolazione dei nuovi *player* operanti nel mercato dei pagamenti e sulla sicurezza delle operazioni, temi che devono essere analizzati parallelamente.

Infatti, i servizi di pagamento offerti dai TPP (*Third Party Provider*) da una parte, accentuano l'aspetto di disintermediazione – nel senso che i TPP si so-

---

http://www.dirittobancario.it; E. ZEPPIERI, *L'implementazione in Italia della nuova direttiva sui servizi di pagamento*, reperibile in internet al seguente indirizzo: http://www.dirittobancario.it; S. BALSAMO TAGNANI, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2,* in *Contr. impr. Eur.*, 2018, 609 ss.; P. MONTELLA, *La Direttiva PSD2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, 2018, II, 129 ss.

[4] Sulle novità introdotte dal d.lgs. n. 218/2017, in generale, cfr. S. VANINI, *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017, n. 218*, in *Nuove leggi civ. com.*, 2018, IV, 839 ss.

[5] Anche la PSD2 è ispirata ai principi di neutralità tecnologica, proporzionalità e trasparenza.

Relativamente al principio di neutralità tecnologica, il Considerando n. 21 della PSD2 ribadisce che «*la definizione di servizi di pagamento dovrebbe essere neutra sotto il profilo tecnologico e consentire lo sviluppo di nuovi tipi di servizi di pagamento, garantendo pari condizioni operative ai prestatori di servizi di pagamento esistenti e ai nuovi prestatori*». Il legislatore comunitario ha, quindi, mantenuto ferma la scelta operata nel 2007 di non identificare rigidamente le modalità tecnologiche che identificano un servizio di pagamento, lasciando libero il prestatore del servizio di elaborare nuovi servizi sempre più efficienti e veloci, nei limiti degli *standard* di sicurezza imposti. Tale scelta è finalizzata a favorire il più possibile l'innovazione tecnologica e a incentivare la concorrenza tra gli operatori.

Per quanto riguarda il principio di proporzionalità, la PSD2 si basa sull'assunto "*same business, same risks, same rules*"; di conseguenza, anche la disciplina dei nuovi *player* presenta regole differenziate e di diversa intensità a seconda dell'attività da questi svolta. L'applicazione concreta di tale principio si riscontra in particolare nelle regole riguardanti l'organizzazione e gli obblighi dei cosiddetti *Third Party Provider* (TPP) a cui sono dedicate regole, in alcuni casi piuttosto stringenti, tese a prevenire i possibili rischi derivanti dall'attività che essi svolgono.

Infine, il principio di trasparenza è un principio cardine del settore bancario-finanziario, in quanto l'informazione è considerata dal legislatore un efficace strumento di tutela per l'utente. In ragione di ciò, la PSD2, così come la precedente direttiva, si pone l'obiettivo di garantire una maggiore chiarezza informativa (Considerando n. 6), introducendo sia specifici obblighi informativi per ciò che riguarda i servizi di pagamento (trasparenza in senso stretto), sia vere e proprie regole di condotta in capo agli intermediari (trasparenza in senso lato). Il principio di trasparenza viene, inoltre, esteso alla circolazione e alla gestione dei dati dei clienti, tema la cui rilevanza emerge soprattutto in relazione al fenomeno dell'*open banking*. Infatti, come si vedrà successivamente, con la PSD2 il legislatore europeo si è dovuto confrontare con le problematiche derivanti dall'introduzione nel procedimento di pagamento di soggetti terzi, i cosiddetti TPP, la cui attività rende necessario lo scambio dei dati dell'utente tra questi e il PSP di radicamento del conto.

stituiscono in parte al PSP di radicamento del conto (ASPSP – *Account Servicing Payment Service Provider*) – d'altra parte, ampliano la frammentazione del procedimento di pagamento, visto che la loro attività è circoscritta ad un determinato segmento del procedimento stesso. La presenza sul mercato di questi nuovi soggetti rende necessario uno scambio di dati e informazioni tra gli intermediari [6], aumentando così i rischi relativi alla sicurezza e alla riservatezza delle informazioni relative agli utenti.

La questione assume particolare interesse se si tiene conto che le informazioni rilevano non solo ai fini del pagamento, ma anche come dati personali dell'utente stesso e, in quanto tali, sono oggetto del recente Regolamento Generale sulla protezione dei dati personali delle persone fisiche n. 679/2016 (*General Data Protection Regulation – GDPR*) [7]. È, quindi, necessario che vi sia un adeguato coordinamento tra le norme specifiche della PSD2 e quelle generali del GDPR; tuttavia, si osserva sin da subito che, sebbene le due discipline siano state emanate quasi contemporaneamente, sono state sollevate alcune perplessità circa il loro rapporto, soprattutto in ordine ai profili dell'utilizzo dei dati personali da parte degli operatori del mercato dei pagamenti e della sicurezza della circolazione degli stessi [8].

Tali questioni rendono necessario un esame preliminare degli aspetti principali delle due normative summenzionate, partendo dalla PSD2, cioè dalla normativa specifica sui servizi di pagamento elettronici.

---

[6] Come opportunamente osservato da V. DE STASIO (*Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Tre-press, 2020, 25 ss.) nell'operazione di pagamento, eseguita tramite il servizio prescelto dall'utente, il procedimento di trasferimento non trasmette più «una sola entità, (ovvero) i fondi che dal conto del pagatore devono pervenire a quello del beneficiario, bensì anche, necessariamente, un'informazione, costituita dall'ordine di pagamento, che dà inizio al procedimento e che nella sua configurazione minima efficace deve contenere un importo, con la valuta che costituisce l'unità di conto numerata dall'importo, e consentire di individuare due conti di pagamento: quello del pagatore, da cui si devono prelevare i fondi nell'importo e nella valuta contenuti nell'ordine, e quello del beneficiario, dove i soldi devono essere accreditati» (27).

[7] Sulle principali novità introdotte con il GDPR, cfr., G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46/CE al nuovo Regolamento europeo*, Torino, Giappichelli, 2016; AA.VV., *La nuova disciplina europea sulla privacy*, a cura di S. Sica, V. D'Antonio e G.M. Riccio, Padova, Cedam, 2016.

[8] Per una prima disamina del problema, v. B. RUSSO, *Tecnologie digitali e tutela dei dati personali: quali possibili impatti sulla PSD2*, in *Riv. dir. banc.*, 2019, 259 ss.

2. *Dalla PSD alla PSD2: i* Third Party Provider *(TPP).*

Come già riferito, l'emanazione della PSD2 è stata la diretta conseguenza del diffondersi, pressoché contemporaneamente all'introduzione della prima Direttiva, di nuovi servizi di pagamento, prestati da soggetti estranei al sistema bancario; questi svolgevano la loro attività senza alcuna regolazione, dato che di essi non si occupava la PSD. Perciò, la PSD2, da una parte, ha preso una posizione favorevole al fenomeno dell'*open banking* [9], dall'altra, ha dettato precise disposizioni per disciplinare l'ingresso nel mercato dei nuovi intermediari e per regolare i servizi da questi offerti, incrementando anche le regole inerenti alla sicurezza dell'operazione, già previste nella PSD [10].

Si deve, innanzitutto, rilevare che la PSD2 ha tipizzato due servizi di pagamento [11]: quello di disposizione di ordini di pagamento, ovvero «un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento» – *Payment Initiation Services Provider* (*PISP*) – [art. 4, n. 15, PSD2 e art. 1, primo comma, lett. b-*bis*), d.lgs. n. 11/2010] e quello d'informazione sui conti, da intendersi come «un servizio *online* che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso uno altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento» – *Ac-*

[9] Con tale locuzione si intende il fenomeno di apertura del sistema bancario a soggetti diversi dalle banche, realizzato attraverso l'obbligo, rivolto alle banche, di mettere a disposizione e condividere con tali soggetti i dati bancari e finanziari degli utenti.

[10] F. CIRAOLO, *I servizi di pagamento nell'era del Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di M.T. Paracampo, Torino, Giappichelli, 2017, 191, evidenzia che è la sicurezza, intesa come affidabilità, autenticità e correttezza delle operazioni, l'ambito in cui emergono maggiormente le problematiche legate al progresso della tecnologia nel campo dei servizi di pagamento, problematiche che si sono acuite con l'ingresso nel mercato dei nuovi operatori, ovvero i TPP.

[11] La PSD2, in applicazione del principio di neutralità tecnologica è rimasta fedele alla scelta presa dal legislatore comunitario con la PSD, di non elaborare una definizione di servizio di pagamento; di conseguenza, si è limitata ad integrare l'elenco già esistente delle attività considerate tali, aggiungendo il servizio di disposizione di ordine di pagamento [art. 1, secondo comma, lett. h-*septies*), n. 7] e il servizio di informazione sui conti [art. 1, secondo comma, lett. h-*septies)*, n. 8]. Per una prima disamina sul tema, cfr. A. ANTONUCCI, *Mercati dei pagamenti: la dimensione digitale*, in *Riv. dir. banc.*, 2018, I, 557 ss.; M. RABITTI, *Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento,* in *Innovazione e regole nei pagamenti digitali, Il bilanciamento degli interessi nella PSD2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Tre-press, 2020, 81 ss.

count Information Services Provider (*AISP*) – [art. 4, n. 16, PSD2 e art. 1, primo comma, lett. b-*ter*), d.lgs. n. 11/2010] [12].

Come si può evincere da queste definizioni, la caratteristica dei nuovi intermediari che possono svolgere tali servizi è che si tratta di soggetti terzi rispetto al rapporto intercorrente tra l'utente e il prestatore di servizi (*Account Servicing Payment Service Provider – ASPSP*) [13] presso il quale il primo ha radicato il proprio conto, tanto è che sono stati denominati *Third Party Provider* (TPP), proprio per sottolineare la loro estraneità alla custodia e alla gestione dei fondi in relazione ai quali il servizio viene eseguito. Tale estraneità costituisce una novità assoluta nel mercato dei pagamenti elettronici; infatti, benchè già con l'adozione della PSD fosse stata riconosciuta a soggetti diversi dalle banche (cioè agli IMEL ed agli IP) la possibilità di svolgere l'attività di prestazione di servizi di pagamento, questa rimaneva inevitabilmente collegata all'esistenza di un conto di pagamento presso lo stesso soggetto che svolgeva il servizio richiesto. Diversamente, l'attività dei TPP riguarda un conto che l'utente già detiene presso un altro intermediario; ciò significa che, come osservato da autorevole dottrina [14], prescindendo la prestazione del servizio dall'esistenza di un conto presso l'intermediario che lo rende, sorgono ulteriori margini di rischio, soprattutto, in ordine alla gestione e alla sicurezza dei dati del cliente.

Si deve, quindi, considerare che i TPP, sebbene svolgano un'attività strumentale a quella di pagamento in senso stretto, rendono più complesso il procedimento, sia perché la conclusione dell'operazione è rimessa alla partecipazione di più intermediari che svolgono attività diverse ma dipendenti l'una dall'altra, sia perché ciò rende necessario uno scambio di dati tra di essi [15]. In

---

[12] Per completezza informativa si deve ricordare che la PSD2 (art. 65) ha disciplinato anche l'attività di conferma della disponibilità dei fondi o *fund checking* sebbene il legislatore comunitario non l'abbia inserita nell'elenco di attività da considerare servizi di pagamento. Tale scelta è probabilmente correlata al fatto che, a differenza dei servizi di disposizione di ordini di pagamento e d'informazione sui conti, si tratta di un'attività che - dietro autorizzazione del titolare della carta – l'emittente della carta stessa effettua a beneficio di se stesso.

[13] Art. 4, n. 17, PSD2 e art. 1, primo comma, lett. g-*bis*), d.lgs. n. 11/2010.

[14] Cfr. M. RABITTI, A. SCIARRONE ALIBRANDI, *Dalla PSD alla PSD2: open banking e servizi di pagamento,* in AA.VV., *Le attuali sfide del sistema bancario. Congiuntura e tecnologia*, in *Osservatorio Monetario*, 1/2019, Milano, 2019, 47 ss.

[15] È stato osservato (V. PROFETA, *I Third Party Provider: profili soggettivi ed oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento, fra PSD2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della consulenza legale della Banca d'Italia*, a cura di F. Maimeri e M. Mancini, Roma, 2019, 52) che la decisione di inserire i servizi di disposizione di ordine di pagamento e di informazione sui conti nell'elencazione dell'art. 1, secondo com-

tale ottica, si spiega come il legislatore, qualora nel procedimento di pagamento intervenga un TPP, si preoccupi di dettare regole anche in ordine al rapporto tra questi e i PSP di radicamento del conto [16]. L'obiettivo, come si vedrà, è quello di garantire un efficace e regolare funzionamento dell'intera catena procedimentale in cui questi soggetti si inseriscono e così assicurare una tutela rafforzata all'utente che decida di avvalersi dei loro servizi [17].

Per quanto riguarda l'avvio dell'attività, la PSD2 ha conservato il regime di riserva, relativamente alla prestazione di servizi di pagamento (art. 114-*sexies*, t.u.b.) [18]; di conseguenza, anche i soggetti che vogliono fornire il servizio di disposizione di ordini di pagamento (PISP) o quello di informazione sui conti (AISP) devono essere previamente autorizzati, in via amministrativa, dall'autorità competente che, nell'ordinamento nazionale, è la Banca d'Italia [19]; ad

---

ma, lett. h-*septies*), t.u.b., nonostante entrambi i servizi abbiano carattere accessorio rispetto all'operazione di pagamento, risponde «all'interesse pubblico di monitorare lo svolgimento delle attività che ne formano oggetto, poiché la tecnologia che li connota, da un lato risulta cruciale per lo sviluppo dei pagamenti digitali, dall'altro pone l'esigenza di implementare i presidi di sicurezza informatica sia per tutelare i fondi, che potrebbero essere aggrediti più facilmente in considerazione del fatto che i nuovi servizi consentono al prestatore che li svolge un accesso diretto e *ab externo* ai conti di pagamento, sia per assicurare la protezione dei dati relativi ai pagamenti resi conoscibili a soggetti terzi diversi sia rispetto al titolare del conto sia rispetto al prestatore presso il quale il conto è radicato».

[16] In proposito, V. DE STASIO, (nt. 6), 25 ss. osserva che mentre la PSD aveva concentrato l'attenzione sulla corretta esecuzione dell'operazione, la PSD2 si concentra sugli aspetti informativi relativi alla trasmissione dei dati dell'operazione di pagamento.

[17] La scelta del legislatore di regolare l'attività dei TPP e il loro rapporto con i PSP di radicamento del conto riveste particolare importanza, soprattutto, in relazione alla tutela dell'utente. Infatti, prima della PSD2, l'assenza di regole in materia non solo impediva la predisposizione di una tutela preventiva in ordine a rischi connessi alla prestazione dei nuovi servizi di pagamento, ma aveva conseguenze anche sul piano della tutela accordata all'utente in caso di esecuzione di un'operazione non autorizzata. Infatti, la comunicazione da parte dell'utente delle proprie credenziali di accesso personalizzate ai TPP, sebbene necessaria all'esecuzione dell'operazione richiesta, configurava una violazione degli obblighi gravanti sull'utente stesso di conservare e non divulgare a terzi i propri codici di accesso, con la conseguenza che, in caso di contestazione di un'operazione non autorizzata eseguita tramite TPP, la banca poteva ridurre o, addirittura, rifiutare del tutto il rimborso dell'operazione all'utente.

[18] Ciò è confermato dall'art. 131-*ter* del t.u.b. (abusiva attività di prestazione di servizi di pagamento) che punisce penalmente chiunque svolga attività di servizi di pagamento in violazione della riserva dell'art. 114-*sexies*, t.u.b. e senza aver previamente ottenuto l'autorizzazione di cui all'art. 114-*novies*.

[19] Per quanto riguarda i PISP, al rilascio dell'autorizzazione consegue l'iscrizione in un apposito registro, liberamente consultabile *on line* e gestito dall'autorità competente di ogni singolo Stato (art. 14, paragrafi 1 e 2, PSD2), che in Italia è la Banca d'Italia.

essa è, inoltre, affidato il compito di controllare la sussistenza dei requisiti necessari per il conseguimento dell'iscrizione [20] e il rispetto permanente degli stessi per tutto il periodo in cui i TPP svolgono la loro attività (art. 23, PSD2). Tuttavia, per gli istituti di pagamento che intendono fornire esclusivamente i servizi in esame, cioè per i TPP, sono previste disposizioni particolari per tener conto del fatto che essi non detengono mai i fondi del cliente.

In particolare, per quanto riguarda i PISP, la domanda di autorizzazione all'esercizio dell'attività deve contenere i requisiti richiesti in generale dall'art. 5 PSD2 (art. 114-*novies*, t.u.b.) e valevoli per tutti gli IP, ma con alcune varianti. Infatti, da una parte, è richiesto un capitale iniziale inferiore [art. 7, par. 1, lett. b), PSD2] [21], dall'altra, è necessario il possesso di un'assicurazione sulla responsabilità civile o analoga forma di garanzia per gli eventuali danni causati nell'esercizio della propria attività (art. 5, par. 2, PSD2 e art. 114-*novies,* co. 1-*bis,* t.u.b.) [22].

Per gli AISP, il legislatore ha previsto ulteriori agevolazioni dato che tali soggetti svolgono un servizio di carattere meramente informativo. Il cuore della disciplina è contenuto nell'art. 33 della PSD2 (art. 114-*speties,* co. 2-*bis,* t.u.b.) che subordina l'ingresso nel mercato all'iscrizione in un albo speciale, iscrizione per la quale sono necessarie solo alcune delle condizioni elencate dall'art. 5 della PSD2 (art. 114-*novies,* co. 1, t.u.b.) [23].

---

[20] In relazione a ciò, è stato sottolineato V. PROFETA, (nt. 15), 60 che, nonostante l'art. 114-*septies,* co. 2-*bis,* t.u.b., parli di iscrizione e non di autorizzazione, alla Banca d'Italia è attribuito un potere di verifica dei requisiti richiesti dalla legge per lo svolgimento dell'attività, potere che non ha carattere meramente ricognitivo, tant'è che, anche con riferimento agli AISP, la Banca d'Italia qualifica il proprio provvedimento come autorizzazione. In sostanza, l'iscrizione non consegue automaticamente alla dichiarazione di possesso dei requisiti da parte dell'AISP ma è subordinata al controllo e all'assenso dell'autorità di controllo; di fatto, anche per quanto riguarda gli AISP è necessaria l'autorizzazione per l'esercizio dell'attività.

[21] Secondo la disposizione contenuta nel punto 1, sez. II del Provvedimento attuativo della Banca d'Italia del 23 luglio 2019 il capitale minimo iniziale richiesto per i PISP è pari ad euro 50.000.

[22] La PSD2 specifica che l'assicurazione deve coprire i danni derivanti da operazioni non autorizzate (art. 73), dalla mancata, inesatta o tardiva esecuzione dell'operazione di pagamento (art. 90), nonché dall'esercizio di regresso da parte di altri prestatori di servizio di pagamento.

[23] Gli AISP sono, infatti, esonerati dall'obbligo di dotarsi di un capitale minimo iniziale [art. 5, par. 1, lett. c), PSD2], né ad essi si applicano le regole (art. 23, par. 3, PSD2) in tema di tutela dei fondi del cliente [lett. b)]. Inoltre, non sono soggetti all'obbligo di rilevazione dei dati statistici relativi alle operazioni e alle frodi [lett. i)], agli obblighi in materia di lotta al riciclaggio e di finanziamento al terrorismo [lett. k)], né devono indicare l'identità delle persone che, direttamente o indirettamente, detengono nel capitale dell'AISP partecipazioni rilevanti [lett. m)] e dei revisori legali dei conti o delle imprese di revisione contabile [lett. o)]. Essi so-

Entrambi i TPP sono soggetti alle norme contenute nella sezione 3 della PSD2 (autorità competenti e vigilanza; art. 114-*quinquies.2*, e art. 114-*quaterdecies*, t.u.b.) e a quelle riguardanti l'onere della prova in relazione ai requisiti informativi (art. 41, PSD2 e art. 126-*bis*, co. 4, t.u.b.). Infine, sono previste disposizioni sugli obblighi informativi nei confronti dell'utente (artt. 45 e 52 PSD2 e 126-*quater*, t.u.b.) e sugli obblighi riguardanti la gestione dei rischi e la sicurezza (artt. 95-98) [24].

3. Segue: *La disciplina in tema di sicurezza [Psd2 e Regolamento (Ue) 389/2018].*

L'ultimo gruppo di disposizioni assume particolare importanza considerata anche la scelta del legislatore di attribuire alla sicurezza la funzione di incoraggiare l'uso e la diffusione dei pagamenti elettronici; ciò emerge in modo ancor più accentuato in relazione ai TPP che si frappongono tra l'utente e il suo PSP, acquisendo al posto di quest'ultimo tutte le informazioni sull'operazione da compiere. Per tale motivo, il legislatore è intervenuto su diversi piani: quello della tutela preventiva, volta ad evitare il verificarsi del danno, e quella della tutela successiva, tesa a ridurre le conseguenze pregiudizievoli per l'utente del servizio [25].

La volontà del legislatore di predisporre un sistema in grado di prevenire i rischi si riscontra sin dalle regole che disciplinano l'ingresso nel mercato dei pagamenti dei TPP, visto che, già nella domanda di autorizzazione o di iscri-

---

no inoltre esenti dall'applicazione delle procedure e delle condizioni contenute nella sezione 1 (disposizioni generali) e nella sezione 2 (tempi di esecuzione e data valuta) del Titolo III della PSD2. Anche per gli AISP, costituisce requisito indispensabile la stipulazione di un'assicurazione per la responsabilità civile professionale a copertura dei danni che possono essere arrecati al PSP di radicamento del conto o all'utente a causa dell'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o dall'uso non autorizzato o fraudolento delle informazioni stesse (art. 5, par. 3, PSD2).

[24] Per quanto riguarda le disposizioni riguardanti la sicurezza, queste sono state trasfuse nel d.lgs. n. 11/2010 – modificato dal d.lgs. n. 217/2018 – e trovano specificazione nelle disposizioni del Regolamento n. 389/2018.

[25] L'idea di fondo, infatti, è che i rischi insiti nell'utilizzo dei pagamenti elettronici non possono essere del tutto eliminati; pertanto, l'impianto legislativo è strutturato, da un parte, imponendo una serie di obblighi di condotta in capo all'intermediario – il cui fine è di far sì che egli predisponga un sistema di sicurezza all'avanguardia e metta in atto accorgimenti in grado di prevenire il verificarsi di un danno –, dall'altra, prevedendo regole relative alla ripartizione della responsabilità e al ristoro del danno subito dall'utente.

zione deve essere presentata una descrizione delle procedure di gestione del rischio adottate [art. 5, par. 1, lett. e), PSD2][26] e di quelle predisposte per il monitoraggio e la gestione degli incidenti relativi alla sicurezza [art. 5, par. 1, lett. f), PSD2][27]; inoltre, la domanda deve essere corredata da un documento attestante la politica di sicurezza adottata sulla base di una valutazione dei rischi relativi ai servizi di pagamento offerti, nonché una descrizione delle misure di controllo e di mitigazione che si intendono mettere in atto per tutelare gli utenti dai rischi inerenti i servizi offerti [art. 5, par. 1, lett. j), PSD2]. In sostanza, l'accesso al mercato dei pagamenti è riservato agli intermediari che dimostrino, ancor prima di aver iniziato la propria attività, di essere in grado di garantire misure di sicurezza idonee a prevenire i rischi insiti nell'attività di prestazione dei servizi di pagamento e procedure per minimizzare gli effetti negativi che eventuali incidenti potrebbero avere sugli utenti[28].

La sicurezza delle operazioni è stata, inoltre, rafforzata intervenendo su due elementi ritenuti fondamentali per prevenire il verificarsi di eventuali incidenti: l'autenticazione – ovvero la procedura che permette al PSP di verificare

[26] Ai sensi dell'art. 95, PSD2 gli Stati membri devono, infatti, assicurare che i PSP istituiscano meccanismi di controllo in grado di gestire i rischi relativi al servizio di pagamento prestato ed elaborino procedure per gestire gli incidenti operativi e la sicurezza. Tale obbligo è rafforzato dal dovere dell'intermediario di comunicare periodicamente all'autorità competente una valutazione aggiornata e approfondita dei rischi operativi inerenti ai servizi di pagamento offerti e dell'adeguatezza delle misure adottate per controllarli e mitigarne gli effetti pregiudizievoli.

[27] Il sistema di gestione adottato dall'intermediario deve essere in linea con quanto disposto dall'art 96 della PSD2. Quest'ultimo prevede un obbligo di notificazione all'Autorità di controllo al verificarsi di un grave incidente operativo o alla sicurezza, in modo tale che questa possa informare l'Autorità Bancaria Europea (ABE) e la Banca Centrale Europea (BCE), soggetti a cui è affidato il compito di valutare la gravità dell'incidente e la rilevanza per gli altri Stati e prendere le opportune decisioni per tutelare il sistema finanziario. Se l'incidente può ledere gli interessi finanziari degli utenti, l'intermediario è tenuto a informarli e a fornire tutte le informazioni riguardanti le misure a loro disposizione per attenuare gli effetti pregiudizievoli derivanti dall'incidente.

[28] In ossequio al principio di proporzionalità, al PSP è, quindi, richiesto di valutare il rischio intrinseco al servizio di pagamento prestato, di adottare le misure ritenute maggiormente in grado, prima di tutto, di evitare il verificarsi dello stesso, e, in secondo luogo, di mitigare le conseguenze che dallo stesso possono derivare. In relazione a ciò, si ricorda che la scelta del sistema di sicurezza riveste particolare rilevanza per l'intermediario in quanto l'adozione di un sistema all'avanguardia e in grado di garantire la massima sicurezza possibile in relazione all'evoluzione della tecnologia è uno dei principali obblighi su di lui gravanti ed è uno degli elementi che vengono presi in considerazione *ex post* per la valutazione della sua condotta nel caso in cui vi sia stata un'operazione non autorizzata.

l'utilizzo di un determinato strumento di pagamento o delle credenziali di sicurezza personalizzate (art. 4, par. 1, n. 29, PSD) – e gli *standard* di comunicazione tra gli intermediari; quest'ultimo aspetto è particolarmente innovativo in quanto regola lo scambio di dati e informazioni tra i TPP e il PSP di radicamento del conto.

a) Per quanto riguarda l'autenticazione, l'art. 97 della PSD2 segna il passaggio ufficiale da un sistema di autenticazione monofattore ad un sistema di autenticazione forte (*Strong Customer Authentication*)[29] ogni qual volta l'utente accede al proprio conto di pagamento [par. 1, lett. a)], dispone un'operazione di pagamento [par. 1, lett. b)] o effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frodi od altri abusi [par. 1, lett. c)]. In realtà, come già segnalato dalla dottrina[30], nel nostro ordinamento, l'adozione di uno *standard* di autenticazione forte era statoa già pretesa dalla giurisprudenza e, in particolare, da quella dell'ABF che, sin dall'introduzione della prima Direttiva sui servizi di pagamento, ha ritenuto l'adozione di un sistema di autenticazione multifattore da parte dell'intermediario elemento di prova che l'operazione era stata correttamente autenticata[31].

---

[29] L'art. 4, par. 1, n. 30 della PSD2, ripreso letteralmente dall'art. 1, primo comma, lett. q-*bis*), d.lgs. n. 11/2010, specifica che per "autenticazione forte" deve intendersi *«un'autenticazione basata sull'uso di due o più elementi classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione»*.

[30] Cfr. V. DE STASIO, (nt. 6) 25 ss.; C. PAGLIETTI, (*Questioni in materia di prova di pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Tre-press, 2020, 43 ss.), la quale mette in evidenza il rilievo attribuito sin da subito al sistema 3D Secure ai fini della valutazione, in sede giudiziale, della condotta dell'intermediario e della sua eventuale responsabilità per l'esecuzione di operazioni non autorizzate.

[31] Cfr., tra le tante, Collegio di Coordinamento, decisione n. 3498 del 26 ottobre 2012; Collegio di Milano, decisione n. 111 del 13 gennaio 2012; Collegio di Roma, decisione n. 263 del 30 luglio 2012; Collegio di Napoli, decisione n. 2121 dell'8 aprile 2014; decisione n. 2609 del 29 aprile 2014, tutte reperibili in internet al seguente indirizzo: http://www.arbitrobancario finanziario.it. Infatti, sin da subito si è consolidato in seno all'ABF un orientamento secondo il quale il sistema a due fattori – ovvero il sistema che per l'autenticazione delle operazioni *on line* affianca all'inserimento del codice identificativo e della *password* un secondo elemento di identificazione tramite il sistema OTP in grado di generare una *password* monouso ogni 60 secondi – era quello più idoneo a garantire l'adeguatezza del sistema di sicurezza allo scopo e agli *standard* imposti dallo sviluppo della tecnologia. Di conseguenza, l'adozione da parte dell'intermediario di tale sistema, sebbene non potesse dare origine ad un automatismo dedut-

La novità, pertanto, non consiste tanto nell'obbligo di adottare tale sistema ma nelle caratteristiche tecniche dello stesso; queste sono state successivamente specificate dal Regolamento (Ue) 389/2018 (*Regulatory Technical Standards*, relativo alle norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri), che ha integrato la disciplina in tema di sicurezza della PSD2 [32] . Infatti, i capi II, III e IV (artt. 5-27) del Regolamento, si occupano delle misure di autenticazione che devono essere impiegate per garantire il massimo livello di sicurezza attualmente possibile; tra queste rilevano le seguenti prescrizioni: i) il collegamento dinamico deve essere collegato ai parametri della transazione [33], nel

tivo circa la negligenza del cliente, era uno degli elementi in grado di provare che l'intermediario aveva adempiuto agli obblighi di condotta impostigli dall'art. 8 del d.lgs. n. 11/2010 e, di conseguenza, implicava una valutazione più severa della condotta dell'utente. Sul punto, cfr. C. PAGLIETTI, (nt. 30), 58, la quale sottolinea che la valutazione della condotta della banca deve essere valutata con diversi criteri di giudizio a seconda che abbia adottato o meno un sistema di autenticazione forte.

A simili conclusioni era giunta anche la giurisprudenza ordinaria, seppur seguendo ragionamenti diversi da quelli dell'Arbitro Bancario Finanziario. La giurisprudenza di merito (cfr. per tutte, Trib. Verona, 2 ottobre 2012, in *Resp. civ. prev.*, 2013, 1284 ss.; Trib. Milano, 4 dicembre 2014, in *Resp. civ. prev.*, 2015, 911 ss., con nota di Frau) riprendendo i principi di carattere generale secondo cui la diligenza esigibile dalla banca ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento, ha ritenuto che la mancata adozione del sistema OTP costituisse una violazione del disposto dell'art. 1176, secondo comma, c.c., in quanto solamente tale tipo di procedura era ritenuto adeguato a prevenire gli eventi pregiudizievoli insiti nell'utilizzo di servizi di pagamento elettronici.

[32] L'art. 98, par. 1, PSD2, infatti, demandava all'Autorità Bancaria Europea l'elaborazione di norme tecniche di regolamentazione – da presentare alla Commissione -, indirizzate ai prestatori di servizi di pagamento, in cui fossero specificati i requisiti di autenticazione forte del cliente [lett. a)]; le esenzioni dall'adozione del sistema di autenticazione forte [lett. b)]; i requisiti che le misure di sicurezza devono rispettare conformemente all'art. 97 per garantire la tutela della riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti [lett. c)]; i requisiti per gli *standard* di comunicazione comuni e sicuri ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni, nonché dell'attuazione delle misure di sicurezza, tra i prestatori di servizi di radicamento del conto, i prestatori di servizi di disposizione di ordini di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri prestatori di servizi di pagamento [lett. d)].

[33] L'art. 5, par. 1, del Regolamento (Ue) 389/2018 impone agli intermediari di adottare misure di sicurezza che soddisfino i seguenti requisiti: «*a) il pagatore è informato dell'importo dell'operazione di pagamento e del beneficiario; b) il codice di autenticazione generato è specifico per l'importo dell'operazione di pagamento e il beneficiario concordato dal pagatore al momento di disporre l'operazione; c) il codice di autenticazione accettato dal prestatore di servizi di pagamento corrisponde all'importo specifico originario dell'operazione di pagamento e all'identità del beneficiario approvato dal pagatore; d) qualsiasi modifica dell'importo o*

senso che il codice di autenticazione deve essere specifico per alcuni elementi dell'operazione come l'importo e il beneficiario; ii) devono essere adottate almeno due tra le categorie della conoscenza, cioè qualcosa che l'utente conosce [34], del possesso, qualcosa che egli possiede [35] e dell'inerenza, qualcosa che caratterizza la sua persona [36]; iii) tali categorie devono essere contraddistinte dall'indipendenza, in modo tale che la violazione di una di queste non infici l'efficienza del sistema di sicurezza che rimane in ogni caso tutelato dal funzionamento dell'altra categoria adottata [art. 9, par. 1, Regolamento (Ue) 389/2018].

b) L'altro elemento oggetto d'integrazione da parte del Regolamento riguarda gli *standard* aperti di comunicazione tra gli intermediari che devono essere comuni e sicuri. Questo tema può essere affrontato più adeguatamente illustrandolo insieme alle regole che disciplinano il servizio di disposizione di ordini di pagamento e il servizio di informazione sui conti.

Innanzitutto, si deve ricordare che entrambi i servizi effettuati dai TPP operano esclusivamente sui conti di pagamento accessibili *on line* (artt. 66, par. 1, e 67, par. 1, PSD2) e sono attività accessorie rispetto all'esecuzione di un'operazione o alla gestione del conto di pagamento. Infatti, l'attività del PISP può essere considerata esecuzione di una delega che si pone a monte del procedi-

---

del beneficiario comporta l'invalidamento del codice di autenticazione generato". Inoltre, il par. 2, dello stesso articolo specifica che il PSP deve garantire la riservatezza, l'autenticità e l'integrità dei seguenti elementi: "*a) l'importo dell'operazione e il beneficiario durante tutte le fasi dell'autenticazione; b) le informazioni visualizzate al pagatore durante tutte le fasi dell'autenticazione, comprese la generazione, la trasmissione e l'utilizzo del codice di autenticazione*».

[34] I requisiti di tale categoria sono indicati nell'art. 6 del sopra citato Regolamento. In proposito, l'ABE, nel suo documento *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2,* del 21 giugno 2019, sottolinea che possono rientrare in tale categoria, le *password*, i *pin* o le domande di sicurezza, mentre devono esserne esclusi i dettagli della carta di pagamento, il relativo codice di sicurezza e l'indirizzo mail.

[35] L'art. 7 del Regolamento stabilisce i requisiti di questa, categoria che, secondo l'ABE può avere ad oggetto anche un bene non materiale quale un'*app*, oppure può essere costituita dalla prova della generazione di un OTP da parte di un *software* o dalla firma digitale.

[36] Nella categoria dell'inerenza, disciplinata dall'art. 8 del Regolamento, l'ABE fa rientrare la scansione delle impronte digitali o della retina e dell'iride, il riconoscimento vocale o della fisionomia del visto o le dinamiche di digitazione. Come si può facilmente intuire tale categoria, utilizzando elementi relativi a caratteristiche biologiche e comportamentali, non solo è quella più innovativa e legata agli sviluppi della tecnologia, ma, allo stato, è quella che garantisce maggiormente l'inviolabilità del sistema.

mento di pagamento vero e proprio [37], mentre il servizio prestato dall'AISP ha carattere meramente informativo [38]; perciò, né PISP né AISP entrano mai in possesso dei fondi dell'utente, come sottolineato dall'art. 66, par. 3, lett. a), PSD2.

La disciplina che attiene a tali servizi è contenuta rispettivamente negli artt. 66 e 67 della PSD2 (artt. 5-*ter* e 5-*quater*, d.lgs. n. 11/2010) e può essere così riassunta: a) l'esecuzione del servizio è subordinata solamente all'esplicito consenso dell'utente, mentre non è necessario che sussista un preesistente rapporto contrattuale tra il TPP e il PSP di radicamento del conto [art. 66, par. 2 e 5 e art. 67, par. 2 e 4, lett. a), PSD2] [39]; b) la comunicazione tra i TPP e il PSP

---

[37] Il *software* del PISP fa da ponte tra il sito *web* del commerciante/beneficiario e la piattaforma di *on line banking* del PSP di radicamento del conto, assicurando al beneficiario che il pagamento è stato disposto e permettendo di eseguire pagamenti *on line* senza che sia necessario utilizzare la carta di credito. Tali caratteristiche, come evidenziato dal Considerando n. 29 della stessa PSD2, hanno favorito la diffusione di tale servizio nel mondo dell'*e-commerce,* visto che, da una parte, permettono all'utente di eseguire il pagamento senza dover inserire sul sito internet i dati della propria carta di pagamento e dall'altra, consentono al venditore/beneficiario di non aderire al circuito di pagamento di una determinata carta evitando così le spese a ciò connesse.

[38] Gli AISP forniscono informazioni *on line* aggregate su uno o più conti di pagamento permettendo così all'utente di disporre immediatamente di un quadro generale della sua situazione finanziaria in un determinato momento.

[39] Sul punto è stato osservato (B. SZEGO, *I nuovi prestatori autorizzati,* in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Tre-press, 2020,166) che al PSP di radicamento del conto è imposta una "collaborazione forzata" derivante direttamente dalla legge, a cui egli non può opporsi a meno che non ricorrano «giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento da parte di tali soggetti, compresi i casi di ordini fraudolenti o non autorizzati» (art. 68, PSD2 e art. 6-*bis*, d.lgs. n. 11/2010). Ciò è ulteriormente confermato dagli artt. 66 e 67 della PSD2; infatti, il primo impone al PSP di radicamento del conto, una volta ricevuto l'ordine di pagamento, di elaborarlo applicando le stesse condizioni previste per quelli ricevuti direttamente dall'utente [par. 4, lett. c)] e di fornire al PISP tutte le informazioni necessarie all'esecuzione dell'operazione [par. 4, lett. b)]. Il secondo obbliga il PSP di radicamento del conto a trattare le richieste di dati ricevute dall'AISP senza discriminazioni se non per motivi obiettivi [par. 3, lett. b)]. Dalle norme riportate emerge una presa di posizione ben precisa da parte del legislatore comunitario, che è quella di favorire la concorrenza tra operatori, impedendo alle banche – soggetti "più forti" in quanto presso di loro è radicato il conto di pagamento dell'utente – di poter scegliere a quali intermediari e a quali condizioni permettere l'accesso al conto di pagamento del cliente, limitando quindi le possibilità dell'utente di avvalersi di tale servizio. Infatti, se il PSP di radicamento del conto negasse, senza giustificato motivo, l'accesso al TPP potrebbe incorrere in sanzioni per la violazione dei principi della libera concorrenza. Per un approfondimento sul tema della concorrenza tra i prestatori di servizio di pagamento, V. MELI, *Opportunità e sfide per la concorrenza nella disci-*

di radicamento del conto deve essere aperta e sicura, vale a dire che il TPP deve identificarsi presso il PSP di radicamento del conto e che lo scambio di informazioni tra gli intermediari per l'esecuzione dell'operazione deve avvenire secondo canali sicuri [art. 66, par. 3, lett. b), c), d), e par. 4, lett. a), e art. 67, par. 2, lett. b), c), e par. 3, lett. a), PSD2]; c) ai TPP non è concesso accedere, usare o conservare dati diversi da quelli necessari per l'esecuzione dell'operazione, né conservare i dati sensibili relativi ai pagamenti dell'utente [40] [art. 66, par. 3, lett. e), f), g), e art. 67, par. 2, lett. d), e), f), PSD2].

In sostanza, le operazioni mediante TPP sono rimesse all'esclusiva volontà dell'utente del servizio, volontà che deve essere espressa tramite il consenso [41]; in questo modo, il diritto dell'utente di avvalersi di un soggetto terzo trova piena tutela. In ogni caso, all'obbligo imposto al PSP di radicamento del conto di consentire ai TPP l'accesso al conto di pagamento e ai dati ad esso relativi fanno da contraltare, da una parte, la limitazione dell'accesso dei TPP al solo conto di pagamento e per finalità determinate, dall'altra, le regole in tema di ripartizione della responsabilità in caso di effettuazione, tramite PISP, di un'operazione senza autorizzazione (art. 73, par. 2, PSD2) o eseguita in maniera inesatta (art. 90, PSD2) [42]. In proposito, rilevano soprattutto le dispo-

---

plina dei servizi di pagamento, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Tre-press, 2020, 135 ss.

[40] Per dati sensibili relativi ai pagamenti si intendono «*dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate. Per l'attività dei prestatori di servizi di disposizione di ordini di pagamento e dei prestatori di servizio di informazione sui conti, il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti*» (art. 4, par. 1, n. 32, PSD2).

[41] Senza entrare nel merito delle questioni relative alla disciplina del consenso dell'utente, qui si vuole sottolineare che il PSP di radicamento del conto non può eseguire alcun controllo per verificare, prima di permettere l'accesso al conto di pagamento del cliente, se quest'ultimo ha effettivamente autorizzato il TPP ad eseguire l'operazione.

[42] Com'è noto, la PSD prevedeva due fattispecie da cui poteva derivare un danno per l'utente: i) l'esecuzione di un'operazione senza il consenso dell'utente (artt. 60-62); ii) la mancata, tardiva o inesatta esecuzione dell'operazione (artt. 74 e 75). Per entrambe le fattispecie, la disciplina era strutturata in modo da garantire una piena tutela all'utente, facendo gravare sull'intermediario, del pagatore nel caso di operazione non autorizzata, del pagatore e del beneficiario nel caso di operazione non eseguita o eseguita in maniera inesatta, il rischio delle stesse. Su questi aspetti, la PSD2 non ha introdotto alcuna modifica sostanziale ma ha ripreso l'impostazione prevista dalla prima Direttiva per regolare i rapporti tra il PSP di radicamento del conto e il PISP qualora l'operazione non autorizzata o eseguita in maniera inesatta sia stata effettuata tramite l'attività di quest'ultimo.

Diversa è invece la situazione dell'AISP che, come più volte ribadito, svolge un servizio

sizioni riguardanti i rapporti tra gli intermediari che hanno partecipato all'operazione; infatti, nonostante nel caso di operazione eseguita tramite PISP, il PSP di radicamento del conto rimanga comunque l'unico soggetto responsabile nei confronti dell'utente per l'esecuzione di operazioni non autorizzate o eseguite in maniera inesatta (art. 73, par. 2, e art. 90, par. 1, PSD2), nel momento in cui egli corrisponde il rimborso, acquisisce il diritto ad ottenere immediatamente dal PISP l'importo corrispondente alla somma rimborsata all'utente [43]. Infatti, sul PISP grava una presunzione di responsabilità che può essere superata dimostrando che, nell'ambito delle sue competenze, l'operazione è stata autenticata, correttamente registrata e non ha subito le conseguenze di un guasto tecnico o di altri inconvenienti (artt. 73, par. 2 e 90, par. 3, PSD2). Tuttavia, l'assolvimento dell'onere probatorio lo libera da qualsiasi responsabilità e fa sì che il rischio derivante dall'esecuzione di un'operazione non autorizzata ricada in via definitiva sul PSP di radicamento del conto.

Gli elementi di particolare interesse della nuova disciplina riguardano la comunicazione tra gli intermediari e l'utilizzo dei dati relativi ai pagamenti in quanto coinvolgono le tematiche della sicurezza e del trattamento dei dati personali. Relativamente al primo tema, gli elementi di novità riguardano l'obbligo dei TPP di autenticarsi [44] ogni qual volta devono eseguire un'operazione – [artt. 28 e 29, Regolamento (Ue) 389/2018] – consentendo, quindi, al PSP di radicamento del conto di distinguere tra operazioni eseguite tramite TPP e operazioni eseguite direttamente dall'utente [45], e la necessaria adozione di canali sicuri di

meramente informativo e, pertanto, ad esso non è applicabile la disciplina prevista per le operazioni non autorizzate o eseguite in maniera inesatta. Tuttavia, si deve sottolineare che, nonostante, la PSD2 non fornisca alcuna indicazione in merito, sull'AISP gravano obblighi in ordine alla sicurezza del servizio prestato e, di conseguenza, egli potrebbe comunque essere ritenuto responsabile se dal mancato rispetto di tali obblighi derivasse un danno per l'utente.

[43] Sul punto, v. G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dalla PSD2*, in *Riv. banca merc. fin.*, 2018, 627 ss.

[44] L'obbligo di autenticazione viene assolto tramite l'utilizzo di certificati digitali – *Qualified Trust Service Providers (QTSP)* – rilasciati da parte di operatori qualificati la cui disciplina è contenuta nel Regolamento (UE) 910/2014 (Regolamento e-IDAS). I certificati devono garantire la confidenzialità, l'integrità e l'autenticità dei dati e assicurare che essi siano stati inviati dall'effettivo mittente. Per un approfondimento sul tema, cfr. D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in *Quaderni di ricerca giuridica della consulenza legale della Banca d'Italia, Le nuove frontiere dei servizi bancari e di pagamento, fra PSD2, criptovalute e rivoluzione digitale*, a cura di F. Maimeri e M. Mancini, Roma, n. 87/2019, 124 ss.

[45] Prima dell'introduzione della PSD2, infatti, i TPP svolgevano la propria attività facendo ricorso al cosiddetto *screen scraping*, ovvero utilizzavano le credenziali fornite direttamente

comunicazione tra gli intermediari, le cui caratteristiche, come già sottolineato, sono fissate dalle disposizioni del Regolamento n. 389/2018.

Senza entrare nei dettagli tecnici della questione [46], si osserva che, in linea generale e in ossequio al principio di neutralità tecnologica, ai PSP di radicamento del conto è imposto di predisporre spazi aperti di comunicazione con i TPP; questi spazi, secondo quanto specificato dalla normativa regolamentare, sono costituiti da un'apposita interfaccia digitale (*Application Programming Interface – API*) che permette la comunicazione con i TPP e uno scambio sicuro delle informazioni necessarie per l'esecuzione del loro servizio [artt. 30 – 36, Regolamento (Ue) 389/2018].

Per quanto riguarda, invece, il trattamento dei dati personali dei clienti [47], la PSD2, prevede due regole di carattere generale, cioè che il trattamento dei dati personali dei clienti da parte dei PSP è autorizzato se necessario per prevenire ed individuare casi di frode – rimandando, per quel che riguarda l'informativa sul trattamento da fornire all'utente, alla normativa in materia (art. 94, par. 1, PSD2) [48] – e che il trattamento e la conservazione dei dati devono essere funzionali all'esecuzione dell'operazione ed espressamente autorizzati dall'utente (art. 94, par. 2, PSD2).

A tali disposizioni, valevoli per tutti gli intermediari, si affiancano quelle riguardanti solo i TPP. Per questi, come sopra accennato, è stato specificato

---

dall'utente per accedere ai conti di pagamento tramite l'interfaccia predisposta dalla banca; in questo modo, il PSP di radicamento del conto non poteva sapere se l'operazione era stata eseguita dall'utente o da un terzo soggetto. Oggi tale modalità operativa è vietata e i TPP nell'eseguire l'autenticazione devono anche indicare se agiscono in veste di PISP o di AISP. L'identificazione del TTP permette, quindi, l'individuazione dei diversi operatori che hanno partecipato all'operazione, circostanza particolarmente rilevante in ordine ai problemi dell'allocazione del rischio e della responsabilità.

[46] Per un approfondimento, cfr. C. FRIGERIO, *Le nuove tendenze nei servizi di pagamento*, in *Le attuali sfide del sistema bancario, Congiuntura e tecnologia, Osservatorio monetario,* Milano, 1/2019, 38 ss.; D. GAMMALDI, C. IACOMINI, (nt. 44), 124 ss.; A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Psd2*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi della Psd2*, a cura di C. Paglietti e I. Vangelisti, Roma, Roma Trepress, 2020, 13 ss.

[47] Di tale tema, con specifico riferimento ai dati relativi ai pagamenti, si parlerà nel successivo paragrafo.

[48] La PSD2, emanata nel 2015, rimanda alla Direttiva (Ce) 95/46 oggi abrogata dal Regolamento GDPR e, di conseguenza, per ciò che riguarda gli obblighi informativi gravanti sull'intermediario deve farsi riferimento a quest'ultima normativa e al d.lgs. n. 101/2018, emanato per riformare ed adeguare alle nuove disposizioni del Regolamento le norme contenute nel d.lgs. n. 196/2003 (Codice della Privacy).

che l'uso, la conservazione e l'accesso ai dati del cliente deve essere limitato all'esecuzione dell'operazione richiesta; pertanto, non possono essere chiesti dati diversi da quelli necessari all'esecuzione della stessa, né i dati comunicati possono essere utilizzati per fini diversi dal servizio richiesto dall'utente. In particolare, per ciò che riguarda i *dati sensibili relativi ai pagamenti* – ovvero «dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate» [49] – questi non possono essere richiesti, nel caso degli AISP, o conservati, nel caso dei PISP; tali dati, pertanto, sono oggetto di una particolare tutela da parte del legislatore.

Il quadro normativo qui delineato, suggerisce alcune preliminari osservazioni, punto di partenza per successive riflessioni. Innanzitutto, emerge chiaramente la volontà del legislatore di incentivare l'utilizzo di servizi sempre più innovativi e, a tal fine, la PSD2 mira a favorire lo scambio di dati e informazioni tra gli intermediari facilitando il più possibile l'accesso ai conti e ai relativi dati da parte dei TPP. Tuttavia, come già sottolineato, i dati degli utenti non rilevano solamente in ordine al servizio di pagamento prestato dall'intermediario, ma rappresentano una risorsa produttiva nell'ambito dell'attività bancaria/finanziaria, visto che costituiscono un importante strumento per individuare le preferenze di spesa, i gusti, la personalità e le scelte economiche di un individuo, permettendone una profilazione sempre più precisa; di conseguenza, possono essere utilizzati per finalità ulteriori rispetto alla mera esecuzione dell'operazione, nei termini che si preciseranno più avanti.

In quest'ottica, il profilo su cui si vuole porre l'attenzione, in relazione all'interferenza tra la normativa settoriale della PSD2 e quella generale del GDPR, riguarda la sussistenza o meno di limiti al trattamento dei dati personali di cui i PSP e i TPP entrano in possesso in funzione della loro attività.

4. *Dati personali dell'utente dei servizi di pagamento e GDPR.*

Per esaminare correttamente tali questioni è necessario svolgere alcune considerazioni preliminari sul Regolamento n. 679/2016 (GDPR), per chiarire prima quali dati relativi ai pagamenti devono essere considerati dati personali dell'utente, poi quale sia il ruolo assunto rispettivamente dal PSP di radicamento del conto e dai TPP (PISP e AISP) in ordine al trattamento degli stessi

[49] V. art. 4, par. 1, n. 32, PSD2, dove si specifica che in relazione ai PISP e agli AISP il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti.

nel momento in cui l'utente si avvale del servizio di disposizione di ordini di pagamento o di quello di informazione sui conti.

L'attenzione del legislatore al tema del trattamento dei dati personali dell'individuo non è recente [50] e le disposizioni dei precedenti testi normativi sul tema non sono andate esenti da dubbi e critiche [51]. In proposito, si deve sottolineare che l'avvento della tecnologia informatica ha determinato un'evoluzione della nozione di *privacy* e del correlato diritto alla riservatezza, che oggi non possono più intendersi solo come una prerogativa assoluta dell'individuo di impedire che alcune informazioni relative alla sua persona vengano divulgate a terzi, ma devono essere lette tenendo presente l'importanza acquisita dall'informazione in sé nel circuito economico [52]; la condivisione di alcuni

[50] Il diritto alla protezione dei dati personali è stato oggetto di diversi interventi normativi tra i quali si ricorda, innanzitutto, la Direttiva (Ce) 95/46, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La direttiva è stata attuata in Italia con la l. n. 679/1996, successivamente sostituita dal d.lgs. n. 196/2003 (Codice della privacy). La Direttiva apre le porte ad una nuova concezione dei dati personali in quanto riconosce l'importanza che essi rivesto per il funzionamento e lo sviluppo della vita economica e sociale di uno stato. Il quadro legislativo è stato completato dalla Direttiva (CE) 2002/58 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, successivamente modificata dalla Direttiva (Ce) 2009/136.

Il progressivo e rapido sviluppo della tecnologia ha, tuttavia, reso le regole della Direttiva del 1995 inidonee a disciplinare fenomeni come il trattamento automatizzato e a garantire una tutela piena ed efficace della persona fisica; di conseguenza, è emersa l'esigenza di riformare il sistema normativo relativo alla protezione dei dati personali, riforma che si è realizzata con l'emanazione del Regolamento (Ue) 2016/679 (GDPR), attuato in Italia con il d.lgs. n. 101/2018. Sulle tappe normative che hanno segnato la disciplina sul trattamento dei dati personali, cfr. A.R. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali,* in *Contr. impr.*, 2017, 586 ss.

[51] Per un'esaustiva panoramica sull'evoluzione del concetto di *privacy* e dei punti più importanti della disciplina precedente all'introduzione del GDPR, cfr. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. impr.*, 2018, 1098 ss.; più recentemente, ID. *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 3 ss.; M. GIORGIANNI, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato,* in *Contr. impr.,* 2019, 1387 ss..

[52] Come evidenziato da V. CUFFARO, *Il diritto europeo* (nt. 51), 1101, «… l'avvento di Internet con la diffusione dei motori di ricerca e la proliferazione dei social network sono accadimenti che hanno determinato una sostanziale modifica dell'angolo prospettico per ciò che hanno portato al centro dell'attenzione non più quelle informazioni sulla persona che potevano rivestire interesse per la cronaca e che, in quanto notizie, riguardavano un numero ristretto di individui, bensì tutte quelle informazioni, anche minute e di per sé scarsamente significative, che riguardano ognuno e che necessariamente e costantemente vengono messe in circolazione

dati personali dell'individuo è, infatti, necessaria per lo svolgimento di molte attività, sia nel campo scientifico, sia nel campo economico, e per poter usufruire di alcuni servizi (si pensi al cosiddetto *e-commerce*). Di conseguenza, quando si parla di *privacy*, oggi, si deve intendere il diritto dell'individuo non già ad una riservatezza assoluta sulle informazioni che lo riguardano, quanto piuttosto alla possibilità di controllarne l'utilizzo da parte di terzi e ad essere tutelato da eventuali abusi [53].

Il diritto alla protezione dei dati personali, pertanto, non è più «una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità» (Considerando n. 4, GDPR) [54]. Si tratta, quindi, di trovare un bilanciamento tra l'interesse individuale e quelli collettivi [55] non solo nell'ambito

in un sistema economico e sociale che affida all'informatica e a internet lo svolgimento delle attività pubbliche e private».

[53] Il Considerando n. 6 sottolinea che «… *la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi ed organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*».

[54] Sul punto, A.R. RICCI, (nt. 50), 600, chiarisce che il diritto alla protezione dei dati personali è assoluto in quanto è riconosciuto a chiunque, garantito solamente alla persona a cui i dati si riferiscono e vantabile nei confronti di tutti; è relativo nel senso che ad esso possono essere posti vincoli esterni tali da limitare l'esercizio delle pretese della persona. Secondo l'Autrice la relatività non è riferibile al diritto in sé ma al contenuto del diritto che deve essere bilanciato con i valori collettivi e tale bilanciamento può portare ad una restrizione dei poteri riconosciuti al titolare del diritto stesso. In questo senso deve essere interpretato il riferimento alla funzione sociale contenuto nel Considerando n. 4 del GDPR; infatti, la "funzione sociale" diventa il limite alle pretese vantabili dall'individuo in relazione ai propri dati personali e il parametro per coordinare tra di loro le pretese dell'interessato, gli interessi del titolare del trattamento e le esigenze avvertite dalla società.

[55] In relazione a ciò, si ricorda che l'art. 5 del GDPR, titolato Principi applicabili al trattamento dei dati personali, stabilisce espressamente che «*I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza); b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, par. 1, considerato incompatibile con le finalità iniziali (limitazione della finalità); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza); e) conservati in una forma che ne consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a con-*

dell'esercizio delle attività imprenditoriali ed economiche [56] ma anche dell'uso

dizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, par. 1, fatta salva l'attuazione di misure tecniche ed organizzative a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza)» (par. 1). «*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione*)» (par. 2). In proposito, è stato osservato (M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali,* in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 179 ss.), come l'art. 5, indicando le modalità che devono caratterizzare l'esercizio dell'attività di trattamento finisca per individuare veri e propri obblighi per il titolare la cui violazione lo espone all'applicazione di sanzioni.

Il legislatore, pertanto, da un parte riconosce l'utilità economica e sociale dei dati personali – utilità che rende necessario limitare in alcuni casi il diritto dell'individuo alla loro protezione – dall'altro, segna i confini entro cui il trattamento può essere lecitamente eseguito; infatti, le limitazioni al pieno esercizio del diritto alla protezione dei dati possono essere imposte solo se «necessarie allo scopo, commisurate ed adeguate al suo conseguimento, proporzionate nei loro effetti con riguardo sia ai vantaggi sia ai pregiudizi che ne derivano», [in questo senso, A. R. RICCI, (nt. 50), 601].

[56] Secondo il Considerando n. 9 del GDPR, la protezione dei dati personali non può diventare un ostacolo alla libera circolazione dei dati o falsare la concorrenza. Come sottolineato da G. LA ROCCA, (*Trattamento dei dati personali e attività bancaria*, in *Riv. dir. banc.*, 2018, 299 ss.), il legislatore è consapevole che la conoscenza dei dati personali costituisce un elemento molto rilevate nell'esercizio delle attività produttive; in ragione di ciò, il GDPR non si oppone all'utilizzo dei dati personali nell'ambito dell'esercizio dell'impresa, ma focalizza l'attenzione sul diritto di ogni individuo ad un trattamento dei propri dati lecito, corretto e trasparente (sul tema cfr. anche, F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, Cedam, 2018, 107 ss.).

In relazione al problema del bilanciamento tra la prerogativa dell'individuo di mantenere riservate alcune informazioni riguardanti la sua persona e l'interesse all'utilizzo di tali dati nell'ambito dell'esercizio dell'attività economica, cfr. Cass., 17 luglio 2015, n. 15096 (in *Giur. it.*, 2015, 2651, con nota di A. MANTELERO, *Diritto all'oblio e pubblicità nel registro delle imprese* e A.R. RICCI, *Pubblicità nel registro delle imprese e diritto alla protezione dei dati personali. Alcune riflessioni a margine di una recente sentenza di Cassazione, in attesa della decisione della Corte di Giustizia dell'Unione Europea*, reperibile in internet al seguente indirizzo: http://www.giustiziacivile.com, *Approfondimenti*, 2016), in cui l'interesse di terzi ad essere informati sui dati dell'imprenditore, alla cui realizzazione è preposto il registro delle imprese, è stata oggetto di bilanciamento con la pretesa dell'imprenditore, amministratore unico della società fallita, alla cancellazione dei suoi dati dal registro per evitare che la sua immagine subisse un pregiudizio derivante dall'associazione del suo nome alla società fallita. La questione è stata, quindi, sottoposta all'attenzione della Corte di Giustizia Europea (sentenza 9 marzo 2017, C-398/2015, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore*

a fini scientifici dei dati personali (per es. a fini di ricerca e studio in campo sanitario) [57].

Ora, ai fini che qui interessano, si devono, innanzitutto, individuare quali siano i dati utilizzati dai PSP e dai TPP, rientranti nella categoria dei dati personali.

In proposito, l'art. 4, par. 1, n. 1, GDPR, definisce dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)» e chiarisce che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» [58]. Da tale definizione – che mette in rilievo come la principale caratteristica dei dati personali sia quella di fornire informazioni che qualificano e permettono di individuare una persona fisica - si può sin da subito dedurre che i dati relativi ai pagamenti sono dati personali nella misura in cui consentono l'identificazione degli utenti del servizio, cioè del pagatore e del beneficiario. Pertanto, rientrano nella categoria dei dati personali, non solo i dati, non direttamente inerenti ai pagamenti, che identificano il pagatore e il beneficiario del pagamento (ovvero, a titolo esemplificativo, il nome, il numero di telefono, la residenza, l'indirizzo di posta elettronica etc..), ma anche dati specificamente attinenti all'ambito dei servizi di pagamento come l'identificativo unico bancario (IBAN), ovvero «la combinazione di lettere, numeri o simboli che il prestatore di servizi di pagamento indica all'utente dei servizi di pagamento e che quest'ultimo deve fornire per identificare con chiarezza un altro utente del servizio di pagamento e/o il conto di pagamento dell'altro utente del servizio di pagamento per un'operazione di pagamento» (art. 4, par. 1, n. 33, PSD2).

Manni, in *Nuova giur. civ. comm.*, 2016, I, 621, con nota di G. CARRARO, *Pubblicità commerciale e "diritto all'oblio" nella prospettiva dei diritti dell'uomo*) e risolta, nel caso di specie, nel senso che il legittimo interesse dei terzi ad essere informati sulle vicende della società avesse una rilevanza maggiore rispetto alla richiesta dell'amministratore di esercitare il proprio "diritto all'oblio".

[57] Si pensi all'attuale dibattito sull'App "Immuni", elaborata per tracciare i contatti dei soggetti risultati positivi al Covid-19, che ha posto la questione del bilanciamento tra il diritto del singolo a non far conoscere i propri spostamenti e l'interesse collettivo a poter controllare il diffondersi tra la popolazione del virus.

[58] La definizione riportata deve essere integrata con alcuni riferimenti contenuti nei Considerando nn. 30, 57 e 64 che forniscono utili indicazioni per chiarire quali elementi rientrino in tale definizione relativamente agli identificativi e ai servizi *on line*.

La conclusione che i dati relativi ai pagamenti rilevassero come dati personali era stata raggiunta anche dalla giurisprudenza precedente l'introduzione della PSD2; infatti, in diverse pronunce relative a casi di operazioni non autorizzate, l'intermediario è stato condannato ai sensi dell'art. 15, Codice della privacy (d.lgs. n. 196/2003) per essere venuto meno ai propri obblighi professionali e aver permesso un utilizzo illecito dei dati personali del cliente [59].

Un discorso a parte meritano i dati considerati dalla PSD2 *dati sensibili relativi ai pagamenti*, ovvero quei dati ritenuti particolarmente importanti perchè la loro appropriazione da parte di terzi estranei espone l'utente ad un concreto rischio di frode; di conseguenza, il legislatore ha previsto regole particolarmente restrittive per quanto riguarda il loro utilizzo da parte dei TPP [art. 66, par. 2, lett. e) e art. 67, par. 2, lett. e), PSD2]. In proposito, si deve ricordare che l'evoluzione tecnologica ha permesso l'elaborazione di sistemi di sicurezza basati anche su elementi relativi a caratteristiche biologiche dell'individuo (rientranti nella categoria dell'inerenza), come ad esempio le sue impronte digitali. Tale circostanza fa sì che, anche in questo caso, la disciplina di settore

[59] Si segnalano, per la giurisprudenza di merito, Trib. Palermo, 12 gennaio 2012 e Trib. Verona, 15 marzo 2012, entrambe reperibili in internet al seguente indirizzo: http://www.iusexplorer.it, e Trib. Roma, 31 agosto 2016, n. 16211, reperibile in internet al seguente indirizzo: http://www.iusexplorer.it; e per la giurisprudenza di legittimità, Cass., 25 maggio 2016, n. 10638, reperibile in internet al seguente indirizzo: http://www.neldiritto.it, la quale nel ricostruire la responsabilità dell'intermediario ai sensi dell'art. 15, Codice della privacy, sottolinea che essa è coerente con quanto disposto dal d.lgs. n. 11/2010 in ordine all'obbligo dell'intermediario di garantire che i dispositivi di sicurezza e le credenziali personalizzate non siano accessibili a soggetti diversi dal legittimo titolare; Cass., 3 febbraio 2017, n. 2950, reperibile in internet al seguente indirizzo: http://www.dirittobancario.it. In tali vicende, le corti di legittimità, partendo dal rinvio fatto dall'art. 15 del Codice della privacy alla disciplina dell'art. 2050 c.c. avevano individuato nella banca la titolare del trattamento dei dati personali del cliente e l'avevano condannata al risarcimento del danno patito dall'utente per non aver adempiuto ai doveri di sicurezza imposti dall'art. 31 del codice stesso. Sul tema, cfr. R. FRAU, *Responsabilità civile della banca per operazioni di home banking disconosciute dal cliente*, in *Resp. civ. prev.*, 2017, 853; e recentemente, ID., *Il trattamento dei dati personali nell'attività bancaria*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 627 ss.

Le decisioni riportate sono particolarmente interessanti in quanto pongono l'attenzione sul fatto che l'appropriazione indebita delle credenziali personalizzate e dei codici segreti dell'utente può causare non solo l'esecuzione di un'operazione non autorizzata – con le relative conseguenze in termini di riparazione del pregiudizio patito dall'utente secondo le norme specifiche della PSD2 – ma configurare anche una delle fattispecie previste dal par. 2 dell'art, 32, GDPR (ovvero la distruzione, la perdita, la modifica, la divulgazione non autorizzata) o, un utilizzo illecito degli stessi, da cui deriva la responsabilità del titolare del trattamento, ovvero l'intermediario, ai sensi e per gli effetti dell'art. 82, GDPR.

si sovrapponga a quella più generale del GDPR, dato che l'art. 9 di quest'ultimo inserisce i dati biometrici [60] tra le categorie particolari di dati [61], per i quali è previsto un generale divieto di eseguire il trattamento (par. 1), se non nei casi espressamente previsti dal legislatore [par. 2, lett. a-j)]. Pertanto, nel caso in cui il sistema di sicurezza dell'intermediario preveda l'utilizzo di dati biometrici come credenziali di sicurezza personalizzate dell'utente, questi sono soggetti ad una disciplina più restrittiva in quanto, per la PSD2, devono essere inclusi tra i dati sensibili (relativi ai pagamenti) e per il GDPR tra i dati il cui utilizzo, come si vedrà, è in linea di principio vietato.

5. Segue*: il ruolo del PSP di radicamento del conto e dei TPP nel trattamento dei dati personali.*

Un secondo aspetto da chiarire riguarda il ruolo assunto dal PSP di radicamento del conto e dai TPP in ordine al trattamento dei dati personali dell'utente che si avvalga del servizio di disposizione di ordini di pagamento o di quello di informazione sui conti.

Com'è noto, il GDPR ha riformulato la nozione di *titolare del trattamento*, figura fondamentale nella disciplina del trattamento dei dati personali e, perciò, centro d'imputazione d'interessi, decisioni e responsabilità (art. 4, par. 1, n. 7) [62]. La sua presenza è sempre necessaria visto che, salva espressa deroga

---

[60] I dati biometrici sono definiti come «*i dati personali ottenuti da un trattamento tecnico scientifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*» (art. 4, par. 1, n. 14, GDPR). Per un approfondimento sulle caratteristiche tecniche e le questioni giuridiche legate ai dati biometrici, cfr. R. DUCATO, *I dati biometrici*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 1285 ss., la quale sottolinea che, nonostante l'art. 9 sembri limitare l'applicazione di una tutela rafforzata solamente ai dati biometrici finalizzati ad identificare in maniera univoca un individuo, tuttavia, tale tutela dovrebbe essere riconosciuta a tutti i dati biometrici, indipendentemente dalle finalità con essi perseguite, in quanto i dati hanno un collegamento irreversibile con l'identità di ogni singolo individuo.

[61] Sono inoltre considerati dati particolari, quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, i dati genetici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, par. 1, GDPR). Per un approfondimento sul tema, cfr. M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. 2016/679*, in *Nuove leggi civ. comm.*, 2017, 165 ss.

[62] L'art. 4, par. 1, n. 7, GDPR definisce il titolare del trattamento «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri,*

di legge, ogni qual volta vi sia un trattamento di dati di persone fisiche deve essere nominato un titolare. La sua principale prerogativa è l'autonomia, in quanto al titolare è espressamente attribuito l'esclusivo potere di determinare le finalità e i modi del trattamento. Proprio perché è lui a stabilire gli scopi per cui si svolge il trattamento e i metodi per eseguirlo, il legislatore gli impone una serie di obblighi sia di carattere generale sia specifici.

In breve, i primi si desumono dai principi elencati nell'art. 5, par. 1, del GDPR che – come si è accennato – sebbene si riferiscano al trattamento identificano, di fatto, veri e propri obblighi per il titolare [63] al quale è richiesto non solo di osservarli ma anche e soprattutto di essere in grado di provarne il rispetto (art. 5, par. 2) [64]. Tra i principali obblighi specifici, invece, vi sono: quelli di comunicazione e informazione [65] sia nei confronti dell'interessato (artt. 13-22 e art. 34, GDPR) [66] sia nei confronti dell'Autorità Garante (art. 33,

determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli Stati membri».

[63] Gli obblighi del titolare, desumibili dai principi espressi dall'art. 5, in alcuni casi prevedono specifiche prestazioni, come ad esempio il dovere di aggiornare, attraverso cancellazione o rettifica, i dati inesatti dell'interessato, in modo da garantire che le informazioni siano sempre esatte; in altri casi, invece, la norma si limita ad indicare gli obiettivi che devono essere raggiunti, ma senza indicazione dei mezzi da adottare per ottenerli e, di conseguenza, la scelta dei mezzi maggiormente idonei al conseguimento del risultato è rimessa alla valutazione del titolare. Cfr. anche nt. n. 55.

[64] In relazione a ciò rileva il disposto del par. 1 dell'art. 24, GDPR, relativo alla responsabilità del titolare del trattamento, il quale specifica che il titolare del trattamento deve mettere in atto tutte le misure tecniche ed organizzative necessarie per garantire ed essere in grado di dimostrare che il trattamento è avvenuto secondo quanto prescritto dal Regolamento stesso.

[65] Conformemente al principio di trasparenza, le informazioni fornite devono essere facilmente accessibili e chiare in modo da permettere una comprensione facile ed immediata (Considerando n. 58).

[66] La trasparenza – annoverata espressamente per la prima volta nel Regolamento (Ue) 679/2016 – trova concreta applicazione in diversi obblighi imposti al titolare e disciplinati dagli artt. 12 – 22 GDPR. In particolare, in applicazione del principio di trasparenza, il titolare: deve adottare misure adeguate a fornire all'interessato le informazioni previste dagli artt. 13 e 14 (art. 12); deve indicare quali sono le informazioni e i dati a cui l'interessato ha il diritto di accedere (art. 15); deve informare l'interessato del suo diritto a chiedere ed ottenere la rettifica (art. 16) o la cancellazione dei dati che lo riguardano (art. 17) e di ottenere una limitazione al trattamento al ricorrere di determinate circostanze (art. 18); deve comunicare all'interessato eventuali rettifiche, cancellazioni o limitazioni del trattamento effettuate (art. 19). Inoltre, all'interessato è riconosciuto il diritto alla portabilità dei propri dati personali (art. 20); il diritto di opporsi al trattamento dei propri (art. 21) e il diritto a non essere sottoposto ad una decisione

GDPR)[67]; quelli inerenti la sicurezza che riguardano sia la predisposizione di misure preventive atte a garantirne un livello adeguato al rischio (art. 32)[68] sia condotte da porre in essere nel caso in cui vi sia stata una violazione dei dati personali.

basata unicamente su un trattamento automatizzato (art. 22). Sul principio di trasparenza, cfr. M. DELL'UTRI, (nt. 55) 199, il quale sottolinea che «la necessaria trasparenza dell'attività di trattamento significa che il rapporto che questo avvia, tra il titolare o il responsabile e l'interessato, è destinato ad articolarsi nel tempo in un gioco di reciproche interrelazioni, in cui, all'imposizione di obblighi di comportamento, di informazione, di aggiornamento e, in termini più generali, di disponibile apertura del responsabile, fa riscontro la sollecitazione, che il legislatore rivolge all'interessato, a interpretare la rivendicazione della tutela delle proprie prerogative in una forma, o dimensione, che ne richiedono l'attivazione in un quadro di strutturale partecipazione dinamica».

[67] L'art. 33, GDPR, al fine di garantire una tutela rafforzata e permettere alle autorità di controllo dei diversi Stati membri di essere aggiornate sulle violazioni dei dati personali e sui rischi che da essere derivano, impone al titolare di comunicare senza ritardo l'avvenuta violazione. Tale dovere costituisce una specificazione del più ampio obbligo di cooperare con l'Autorità espressamente previsto dall'art. 31, GDPR.

[68] Come già evidenziato, la sicurezza costituisce uno dei principi che devono ispirare il trattamento dei dati da parte del titolare che, per tutto il tempo in cui i dati rimangono in suo possesso, deve garantire la protezione degli stessi da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale [art. 5, par. 1, lett. f)]. Anche la disciplina del GDPR è, quindi, ispirata al principio "*same, business, same risk, same rules*" e, infatti, il primo paragrafo dell'art 32 specifica che il titolare nell'adottare le misure tecniche ed organizzative in grado di garantire un livello di sicurezza adeguato al rischio, deve tenere presenti la natura, l'oggetto, il contesto e le finalità del trattamento e del relativo rischio che può avere diversa probabilità e gravità; la valutazione di tali elementi deve essere svolta sin dal momento dell'ideazione e della progettazione di un trattamento così come esplicitamente disposto dall'art. 25 del GDPR. Infatti, come più volte sottolineato, uno degli elementi su cui si basa la disciplina della sicurezza del GDPR è costituito dalla tutela preventiva, basata sulla logica precauzionale di prevenzione del rischio; infatti «il focus normativo, precedentemente incentrato sulla legittimità del trattamento e sull'auto-determinazione del soggetto si è spostata sulla gestione del rischio» (C. CUPELLI, F. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice privacy dal d.lgs. n. 101/2018*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 1111; per un approfondimento sul tema della tutela preventiva, cfr. anche F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei* sistemi, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 775 ss.; A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Le riforme del diritto italiano*, collana diretta da G. Finocchiaro, Bologna, Zanichelli, 2017, 3101 ss.; G. CODIGLIONE, *Risk based approch e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di S. Sica, V. D'Antonio, G. M. Riccio, Padova, Cedam, 2016, 55 ss.)

A tal proposito, al titolare è attribuito il potere di designare, nel caso sia necessario, un *responsabile del trattamento*, ovvero «la persona fisica o giuridica, l'autorità pubblica, il servizio o l'ente che tratta dati personali per conto del titolare del trattamento» (art. 4, par. 1, n. 8, GDPR). La definizione evidenzia che la principale caratteristica dell'attività svolta da questo soggetto è la strumentalità [69]; il responsabile, infatti, non è una figura autonoma ma deve svolgere la propria attività seguendo le finalità e le istruzioni impartite dal titolare e, di conseguenza, può essere considerato un collaboratore ausiliario di quest'ultimo, in nome e per conto del quale agisce (artt. 28-30, GDPR) [70]. Tale

[69] Il rapporto tra titolare e responsabile del trattamento si instaura tramite contratto o altro atto giuridico dell'Unione europea, redatto in forma scritta o in formato elettronico, il cui contenuto è in parte indicato direttamente dal legislatore. Infatti, l'art. 28, par. 3, stabilisce che con il contratto vengono indicati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritto del titolare del trattamento. In particolare, il contratto deve prevedere che il responsabile del trattamento: «*a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi d'interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiamo un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere ad un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato*». Le disposizioni riportate evidenziano come il responsabile svolga un'attività di ausilio e supporto a quella del titolare e, pertanto, non autonoma ma indirizzata dalle direttive del titolare, che risponde anche del trattamento eseguito tramite il responsabile.

[70] Il responsabile del trattamento, sebbene non sia una figura sempre necessaria come quella del titolare, riveste indubbiamente un'importanza pratica considerevole; in ragione di ciò, l'art. 28 del Regolamento (Ue) 679/2016 riserva tale ruolo a soggetti in possesso di specifiche competenze tecniche in grado di garantire che il trattamento venga effettuato conformemente al GDPR. Per un

ruolo trova ulteriore conferma nel fatto che la determinazione da parte del responsabile delle finalità e dei mezzi del trattamento ha come conseguenza l'assunzione da parte sua della veste di titolare del trattamento (art. 28, par. 10, GDPR) con l'applicazione della relativa disciplina. In sostanza, il responsabile che non abbia adempiuto ai propri obblighi di collaborazione nei confronti del titolare o si sia discostato dalle indicazioni ricevute è ritenuto dal legislatore un titolare di fatto.

L'individuazione dei ruoli rivestiti dai soggetti coinvolti nel trattamento dei dati personali dell'interessato rileva, soprattutto, ai fini dell'eventuale ripartizione di responsabilità nei rapporti interni. Infatti, mentre, per garantire una tutela rafforzata dell'interessato, l'art. 82, paragrafi 1 e 4, GDPR, prevede una responsabilità solidale del titolare e del responsabile del trattamento nei confronti dell'interessato che abbia subito un danno a causa dell'illegittimo trattamento, nei rapporti interni rileva il ruolo rivestito. Infatti, il par. 2 del medesimo articolo specifica che il titolare risponde del danno cagionato dal suo trattamento che violi le norme del GDPR, mentre il responsabile può essere chiamato a rispondere del danno patito dall'interessato solo se abbia violato gli obblighi su di lui gravanti *ex lege* o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal titolare.

Pertanto, il titolare è responsabile sia del trattamento illegittimo che egli abbia effettuato direttamente, sia di quello che altri abbiano effettuato per suo conto, in quanto è al titolare che il GDPR attribuisce il potere decisorio sulle finalità e sui mezzi del trattamento; di conseguenza, il responsabile che si sia attenuto alle disposizioni impartitegli dal titolare e ai propri obblighi di legge, potrà agire in via di regresso nei confronti del titolare, ai sensi dell'art. 82, par. 5, GDPR, nel caso in cui abbia dovuto pagare il risarcimento del danno patito dall'interessato [71].

---

approfondimento sulla figura del responsabile del trattamento e sui suoi rapporti con il titolare, cfr. D. FARACE, *Titolare e responsabile*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 73 ss.; L. GRECO, *I ruoli: titolare e responsabile*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali, Le riforme del diritto italiano*, opera diretta da G. Finocchiaro, Bologna, Zanichelli, 2017, 251 ss.; E. PELINO, *I soggetti del trattamento*, in *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, di E. Pelino, L. Bolognini, C. Bistolfi, Milano, Giuffrè, 2016, 120 ss.; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi. civ.comm.*, 2017, 377.

[71] La scelta del legislatore di esimere da responsabilità il responsabile che si sia attenuto alle disposizioni impartitegli dal titolare integra e completa la disposizione, contenuta nell'art. 28, par. 10, la quale attribuisce al titolare, che si sia discostato dalle indicazioni del titolare, il ruolo di titolare del trattamento. Infatti, come già sottolineato, il titolare è l'unico soggetto a

Relativamente all'identificazione degli intermediari (PSP di radicamento del conto e TPP) che possono assumere la veste di titolare del trattamento, è indubbio che nel momento in cui l'utente apre un conto corrente o un conto di pagamento presso un PSP, questi diventa il titolare del trattamento dei dati personali forniti dal cliente, mentre è più difficile individuare immediatamente il ruolo assunto dal TPP. Infatti, come più volte sottolineato, ai fini dell'esecuzione dell'operazione da parte dei TPP non è necessaria la sussistenza di un rapporto contrattuale tra questi e il PSP di radicamento del conto, ma è sufficiente che l'utente esprima il proprio consenso all'esecuzione dell'operazione. Ciò porta ad escludere che i TPP possano essere considerati, seppure limitatamente al momento dell'esecuzione dell'operazione, come collaboratori del PSP di radicamento del conto e, in quanto tali, assumere il ruolo di soggetti responsabili del trattamento. Tuttavia, i TPP, per quanto soggetti autonomi, svolgono un'attività accessoria a quella dei PSP e, sebbene l'operazione eseguita sia unica, si rende necessaria la collaborazione di entrambi gli intermediari; si instaura, perciò, un rapporto occasionale, che trova fonte nella volontà dell'utente e nella legge, e in cui ogni intermediario esegue il segmento di operazione di sua competenza. In altre parole, i due soggetti rimangono indipendenti uno dall'altro, nonostante l'obbligo di collaborazione.

Se questo è il quadro, si può ipotizzare che, nel momento in cui l'utente dispone un ordine di pagamento tramite PISP o si avvale dell'attività dell'AISP, anche questi soggetti diventino titolari del trattamento, così come il PSP di radicamento del conto.

A questo punto, l'alternativa è se si debba prospettare la costituzione di un rapporto di contitolarità, così come previsto dall'art. 26, GDPR o se si debba ritenere che gli stessi soggetti siano entrambi titolari ma autonomamente. L'art. 26, infatti, prevede che, nel caso in cui il trattamento sia affidato a più soggetti, questi determinino congiuntamente le finalità e i modi dello stesso [72] e che le ri-

cui è attribuito il potere di prendere decisioni circa le finalità e i mezzi per eseguire il trattamento e, di conseguenza, su di lui gravano i rischi connessi alle scelte prese nell'ambito dello svolgimento della propria attività.

[72] D. FARACE, (nt. 70), 752, riferisce che la contitolarità può essere solidale quando le finalità e i mezzi sono totalmente condivisi dai titolari, o parziaria, quando le decisioni relative al trattamento sono prese congiuntamente ma i contitolari partecipano con finalità e con mezzi distinti. Relativamente a quest'ultima ipotesi, si è posto il dubbio se la situazione di contitolarità abbia come conseguenza un'automatica estensione delle finalità di ogni titolare agli altri; la risposta preferibile sembra essere quella negativa [cfr. E. PELINO, (nt. 70), 137] e, pertanto, si deve ritenere che ad ogni titolare è riconducibile la propria finalità. Sul complesso rapporto tra contitolari, cfr. anche L. M. SALVIATI, *Sub. Art. 26*, in *GDPR e normativa privacy. Commentario*, a cura di M. Riccio, G. Scorza, E. Belisario, Milano, Wolters Kluwer, 2018, 260.

spettive responsabilità in merito all'osservanza delle norme del Regolamento siano poi fissate tramite un accordo interno, che rifletta in maniera trasparente i ruoli e i rapporti con gli utenti/interessati, accordo che deve essere messo a conoscenza di questi ultimi, in modo da permettere loro di individuare i soggetti che hanno eseguito il trattamento e i relativi obblighi. In relazione a ciò, si deve osservare che il contratto non ha funzione costitutiva del rapporto di contitolarità ma serve, invece, a individuare i rispettivi obblighi dei contitolari e a ripartire tra gli stessi le relative responsabilità (art. 26, par. 1). Il rapporto di contitolarità, pertanto, nasce dalla condivisione delle finalità o dalle comuni decisioni circa le modalità per eseguirlo e, di conseguenza, l'accordo tra i contitolari ha efficacia solamente nei rapporti interni, non rilevando nei confronti dell'interessato l'assetto organizzativo prescelto. Tale conclusione è confermata dal fatto che il legislatore offre comunque all'interessato la possibilità di esercitare i propri diritti nei confronti dell'uno o dell'altro titolare, indipendentemente da quanto stabilito nell'accordo stesso (art. 26, par. 3, GDPR) [73], senza che il titolare verso il quale egli ha agito possa opporgli la ripartizione di responsabilità in esso dedotta.

La contitolarità, quindi, ricorre qualora il PSP di radicamento del conto e i TPP determinino congiuntamente, almeno in parte, le finalità e i modi del trattamento dei dati dell'utente e raggiungano un accordo, circoscritto all'attività di trattamento dei dati personali, per stabilire i rapporti con l'utente e la ripartizione delle eventuali responsabilità (art. 26, par. 2). In mancanza di risultanze in tal senso, è da ritenere che ogni intermediario abbia autonomamente stabilito le finalità e i modi per eseguire il trattamento dei dati personali dell'utente e ciò anche in ragione del fatto che dalla disciplina di settore emerge chiaramente l'indipendenza di tali soggetti l'uno dall'altro, sia per ciò che riguarda l'aspetto organizzativo, sia per ciò che riguarda i rapporti con l'utente; di conseguenza, non vi è motivo di ritenere che – nonostante essi collaborino per una comune finalità, ovvero l'esecuzione dell'operazione richiesta dall'utente – vi sia una condivisione di finalità o strumenti del trattamento o di decisioni tra il PSP di radicamento del conto e i TPP [74] e, quindi, una situazio-

[73] Sul punto, cfr. L. M. SALVIATI, (nt. 72), 260.

[74] Il fatto che la contitolarità non sia determinata dall'accordo, ma si evinca dalle circostanze di fatto, rende più difficile per l'interessato distinguere tra le due fattispecie, soprattutto nel caso in cui la titolarità sia autonoma ma connessa (come nel caso di TPP e PSP di radicamento del conto). In relazione a quest'ultima si condivide l'opinione della dottrina (cfr., G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012, 84) secondo cui in tale circostanza sarebbe utile che i titolari scegliessero tra di loro un referente cui l'interessato possa fare capo.

ne di contitolarità nel trattamento dei dati personali dell'utente.

In sintesi, nel momento in cui l'utente si avvale dell'attività di un PISP o di un AISP, anche questi ultimi diventano titolari del trattamento dei suoi dati personali e, di conseguenza, rispondono del trattamento dei dati di cui vengono a conoscenza in ragione della loro attività; dati che essi riceveranno in parte dall'utente stesso, in parte dal PSP di radicamento del conto su cui il servizio viene eseguito [75]. La collaborazione tra PSP di radicamento del conto e TPP legittima il trasferimento di dati dall'uno all'altro ma non determina, in linea di principio, una contitolarità nel trattamento, trattamento di cui rimangono entrambi titolari autonomi.

Tale conclusione ha dei riflessi non trascurabili, non nei rapporti esterni quanto in ordine all'eventuale ripartizione di responsabilità tra gli intermediari che intervengono nell'esecuzione del servizio richiesto. Infatti, nel caso in cui l'utente/interessato lamenti un pregiudizio dovuto alla violazione delle norme in tema di trattamento dei dati personali non rileva nei suoi confronti che il trattamento sia stato eseguito in regime di contitolarità oppure autonomamente dai singoli titolari, dato che vige il regime di solidarietà previsto dal par. 4 dell'art. 82, GDPR. Perciò all'utente è riconosciuta comunque una tutela rafforzata visto che egli potrà avvalersi della solidarietà anche quando vi sia una situazione di contitolarità ed egli sia, in ipotesi, in grado di individuare il contitolare a cui è riconducibile il trattamento che gli ha causato il danno.

Diversa è la situazione nei rapporti interni. Infatti, mentre nel caso della contitolarità, disciplinato dall'art. 26, i rispettivi obblighi e le rispettive responsabilità sono fissate nell'accordo, nel caso di trattamento autonomo da parte di più titolari si applicherà la disciplina dell'art. 82, par. 5 [76]. Questa si limita a stabilire che il pagamento dell'intero risarcimento da parte di uno dei titolari fa sorgere il suo diritto a reclamare nei confronti degli altri titolari coinvolti «la parte del risarcimento corrispondente alla loro parte di responsabilità». In relazione a ciò, si deve osservare che, in mancanza di indicazioni da parte del legislatore comunitario sui criteri da utilizzare per ripartire le responsabilità tra i titolari e di una

[75] La circostanza che il TPP riceva i dati direttamente dall'utente o dal PSP di radicamento del conto rileva ai fini dell'applicazione della disciplina riguardante l'informativa che il TPP/titolare deve fornire all'utente/interessato in relazione al trattamento dei dati personali. Nel primo caso, infatti, saranno applicabili le disposizioni dell'art. 13, nel secondo, invece, quelle contenute nell'art. 14, GDPR.

[76] Per un approfondimento sulla natura della responsabilità dei soggetti coinvolti nel trattamento e sul risarcimento, v. M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 1017 ss.

regolazione pattizia dei criteri stessi, si deve far riferimento alle norme di diritto comune e in particolare, con riferimento all'ordinamento nazionale, all'art. 1298, secondo comma, c.c. ai sensi del quale, le parti di ciascun obbligato solidale si presumono uguali se non risulta diversamente.

In entrambi i casi, quindi, il titolare che ha pagato l'intero risarcimento potrà agire in via di regresso nei confronti degli altri titolari partecipanti, ma con una significativa differenza. Infatti, nel caso di contitolarità *ex* art. 26, egli dovrà solamente dimostrare di aver adempiuto agli obblighi attribuitigli, in quanto l'entità delle singole responsabilità è stata già determinata nell'accordo; nel caso di titolari autonomi, invece, la presunzione di legge fa sì che il titolare possa chiedere ad ogni titolare coinvolto solamente la propria quota. Di conseguenza, per vincere la presunzione di legge, egli dovrà provare l'esclusivo o maggior grado di responsabilità di uno o più degli altri titolari coinvolti, secondo il principio di colpevolezza [77].

In conclusione, nel caso in cui l'utente si avvalga dell'attività dei TPP, si può ragionevolmente ipotizzare che si sia in presenza di titolarità autonoma sebbene connessa, stante la necessaria collaborazione tra questi e il PSP di radicamento del conto. Pertanto, nel caso in cui l'utente/titolare, subisca un danno conseguente al trattamento effettuato da entrambi gli intermediari egli potrà agire per l'intero ammontare del danno nei confronti dell'uno o dell'altro ai sensi dell'art. 82, par. 4, GDPR; l'intermediario che ha pagato il risarcimento avrà, poi, il diritto di agire in via di regresso nei confronti dell'altro intermediario ai sensi del par. 5 dell'art. 82 e nei termini sopra esaminati.

6. *Utilizzo e limiti al trattamento dei dati personali da parte degli intermediari.*

Sulla base delle conclusioni raggiunte, si può ora analizzare il problema dell'utilizzo e degli eventuali limiti al trattamento dei dati personali da parte dei PSP.

[77] Com'è noto, secondo gli orientamenti più accreditati, e per influenza della legislazione di origine comunitaria, si è assistito ad una riformulazione del concetto di colpevolezza, non più incentrato sulla valutazione di una condotta poco attenta ma sull'organizzazione poco efficiente del soggetto su cui gravano precisi obblighi riguardanti l'assetto organizzativo della propria impresa. In altre parole, la responsabilità di un soggetto che svolge attività d'impresa non deriva da una sua determinata condotta, ma dalle scelte in ordine all'organizzazione della propria impresa; pertanto, la condotta colpevole è identificata con la mancata adozione dei mezzi e di un'organizzazione idonei a prevenire i rischi correlati all'attività svolta.

Come precedentemente appurato, la normativa specifica sui servizi di pagamento della PSD2, circoscrive l'utilizzo dei dati dell'utente a ciò che è necessario per l'esecuzione del servizio e lo subordina al suo esplicito consenso, rimandando, per ciò che riguarda l'informativa e qualsiasi altro trattamento alla Direttiva (Ce) 95/46 all'epoca vigente ed oggi abrogata e sostituita dal Regolamento (Ue) 679/2016. Oltre a queste vengono in considerazione anche le norme specifiche per i PISP e gli AISP che restringono ancor di più le possibilità dei TPP di chiedere informazioni e dati non necessari all'esecuzione dell'operazione e ne vietano un utilizzo per fini diversi dall'esecuzione dei propri impegni contrattuali.

La disciplina di settore, pertanto, prevede un regime piuttosto rigido per gli intermediari; tuttavia, nella prassi si riscontra un utilizzo ben più ampio da parte dei PSP e dei TPP dei dati degli utenti, utilizzo la cui liceità deve essere verificata facendo riferimento anche alle disposizioni del GDPR.

In proposito, l'art. 6, GDPR, contempla una serie di circostanze (le cosiddette basi giuridiche) che legittimano il trattamento dei dati personali della persona fisica (consenso dell'interessato, esecuzione di un contratto, obbligo legale, salvaguardia di interessi vitali dell'interessato o di altra persona fisica, esecuzione di compiti d'interesse pubblico o connessi all'esercizio di pubblici poteri, interesse del titolare o di terzi). Fra queste assume un ruolo residuale il consenso. Infatti, ogni qual volta il trattamento non sia ricollegabile ad una delle altre basi giuridiche specificamente contemplate, il trattamento è ammesso previo consenso dell'interessato, purché esso sia riferito a finalità specifiche e determinate [78].

Venendo, quindi, all'attività dei PSP e dei TPP, tre sono le circostanze che implicano normalmente il trattamento dei dati personali dell'utente.

i) La prima è quando il trattamento dei dati personali dell'utente è necessario per l'esecuzione di un contratto di cui l'interessato è parte [art. 6, par. 1, lett. b)]; in questo caso, il trattamento può essere effettuato senza chiedere il suo preventivo consenso – da ritenersi implicito nella sottoscrizione del contratto – ed è funzionale alla realizzazione di quanto in esso stabilito. Di conseguenza, l'oggetto del contratto, ovvero l'esecuzione del servizio richiesto

[78] Il titolare deve optare per la base giuridica più idonea al trattamento che vuole porre in essere; la scelta ha un'importanza pratica non indifferente visto che ogni base giuridica risponde a condizioni specifiche e ha effetti differenti sui diritti dell'interessato. Il titolare deve, quindi, previamente valutare le finalità perseguite e gli obblighi su di lui gravanti in base alla scelta effettuata e ciò anche in considerazione del fatto che egli deve essere in grado di dimostrare la correttezza della propria scelta.

dall'utente, costituisce il limite entro cui può essere effettuato il trattamento e l'elemento da considerare per valutare l'adeguatezza, la pertinenza e la stretta necessità del trattamento stesso [79]. Tale base giuridica è, quindi, in linea con le disposizioni della PSD2 che circoscrivono l'accesso, l'utilizzo e la conservazione delle informazioni e dei dati, a quelli necessari per l'esecuzione del servizio che sia stato richiesto sia ai PSP sia ai TPP.

In proposito, si deve, però, osservare che mentre per il GDPR la legittimazione contrattuale è elemento sufficiente, in linea di principio, a giustificare l'utilizzo e la conservazione dei dati dell'utente – richiedendosi il consenso esplicito dell'interessato solamente in riferimento al trattamento dei dati rientranti in particolari categorie (art. 9, GDPR) oppure in riferimento alla profilazione (art. 22, GDPR) – la PSD2, invece, richiede l'esplicito consenso in ogni caso, ovvero anche per un utilizzo dei dati funzionale all'esecuzione delle obbligazioni contrattuali relative all'esecuzione del servizio richiesto (art. 94, par. 2, PSD2) [80]. Le disposizioni riportate sembrano apparentemente inconciliabili ma il contrasto è ricomponibile sulla base dell'art. 64, PSD2 che subordina la legittimità dell'operazione di pagamento al previo consenso dell'utente. Tale disposizione può essere interpretata nel senso che il consenso, richiesto per ogni operazione di pagamento, assorbe quello richiesto dal successivo art. 94, par. 2, PSD2. Seguendo tale interpretazione, il consenso dell'utente all'esecuzione dell'operazione sarebbe, quindi, sufficiente a legittimare l'utilizzo dei suoi dati personali da parte dell'intermediario in ragione dell'esecuzione del servizio richiesto e ciò eliminerebbe il contrasto con quanto disposto

[79] In relazione a ciò, è stato sottolineato [M. DELL'UTRI, (nt. 55), 222] che un problema si potrebbe porre quando il trattamento dei dati, pur non essendo strettamente necessario all'esecuzione della prestazione contrattuale, ne consente comunque un'esecuzione migliore.

[80] In proposito, la dottrina [M. RABITTI, A. SCIARRONE ALIBRANDI, (nt. 14), 57] partendo dal presupposto che al consenso è assegnato un ruolo centrale sia dalla disciplina della PSD2 sia da quella del GDPR, ha posto la questione circa il corretto significato attribuitogli dalle due discipline e si è domandata se il consenso richiesto dalla PSD2 per l'operatività dei TPP sia sufficiente a legittimare anche l'attività di trattamento dei dati personali degli utenti conformemente a quanto disposto dal GDPR. Sul tema, cfr anche D. HELGADOTTIR, (*The conflict concerning data sharing under PSD2 and obtaining consent to share such data under GDPR,* reperibile in internet al seguente indirizzo: http://www.law.oc.ac.uk/business-law-blog) che, dopo aver analizzato il consenso previsto dalla PSD2 e quello previsto dal GDPR, giunge alla condivisibile conclusione che la PSD2 non può essere considerata *lex specialis* rispetto al GDPR, sottolineando che «*Payment service providers must both fulfil the explicit consent requiremente under PSD2 and be able to rely on one of the other five lawful bases available under the GDPR for processing personal data*».

dall'art. 6, par. 1, lett. b), GDPR [81]. In ogni caso, qualsiasi ipotetico contrasto dovrebbe superarsi con l'applicazione di quest'ultima disposizione, in quanto il rinvio alla normativa sul trattamento dei dati personali – che è contenuto nel primo paragrafo dell'art 94, PSD2 - deve intendersi riferito al GDPR, il quale regola l'intera materia ed è temporalmente successivo alla PSD2.

ii) La seconda circostanza riguarda la possibilità degli intermediari di trattare i dati degli utenti per prevenire, indagare ed individuare casi di frode nei pagamenti (art. 94, par. 1, PSD2). In relazione a ciò, un'indicazione circa la base giuridica che legittima l'intermediario al trattamento viene fornita dal Considerando n. 47 del GDPR che, con riferimento ai casi in cui è riscontrabile un interesse del titolare tale da giustificare il trattamento [art. 6, lett. f), GDPR], menziona espressamente la prevenzione delle frodi [82]. L'attività di prevenzione è, quindi, l'elemento che può consentire di eseguire il trattamento senza il preventivo consenso dell'interessato, anche se tale circostanza non è di per sè sufficiente a rendere legittimo il trattamento. In proposito, il titolare deve effettuare un preventivo bilanciamento tra il suo interesse e quello della persona a non vedere compromessi i propri diritti e libertà fondamentali [83]. Una volta effettuato il bilanciamento, il trattamento può, però, essere eseguito

[81] In relazione a ciò, si segnala anche l'intervento chiarificatore dello *European Data Protection Board* (EDPB), organismo indipendente il cui scopo è quello di garantire un'applicazione coerente del GDPR e di coordinare l'attività dei garanti nazionali dell'Unione; a tale scopo formula raccomandazioni, stabilisce *standard* comuni per gli Stati membri, emette pareri su questioni tecniche per gli Stati e per la Commissione europea. Quest'organismo, con lettera del 5 luglio 2018, ha precisato che il consenso di cui all'art. 94, par. 2, PSD2, ha natura contrattuale e fa, quindi, riferimento solamente al rapporto instauratosi tra utente e prestatore del servizio. Esso ha, quindi, effetto limitato al tipo di servizio di pagamento richiesto e solo per ciò che riguarda quest'area di applicazione sostituisce il consenso preteso dal GDPR che ha carattere più generale. I due testi normativi, pertanto, concorrono ognuno per ciò che riguarda l'oggetto della propria regolamentazione.

[82] Tale base giuridica può essere adottata, quindi, anche per il trattamento eseguito per la messa in atto delle misure di sicurezza e, nel caso delle banche, per valutare il merito creditizio del cliente. In entrambi i casi, infatti, l'intermediario persegue un proprio interesse ritenuto legittimo dall'ordinamento; in ogni caso, resta ferma l'impossibilità di eseguire il trattamento nel caso in cui questo pregiudichi i diritti o le libertà fondamentali dell'utente/interessato.

[83] Il titolare è chiamato a svolgere un'attenta disamina degli interessi in gioco, tenendo al primo posto i diritti e le libertà fondamentali dell'interessato per evitare che, in un'eventuale valutazione *ex post*, il trattamento possa essere ritenuto illegittimo. Tale valutazione rientra nell'obiettivo del GDPR di responsabilizzare il titolare del trattamento; infatti, prima dell'introduzione della nuova normativa, il bilanciamento degli interessi delle parti era affidato all'Autorità garante del trattamento dei dati personali [art. 24, lett. g), Codice della privacy].

solo entro i limiti delle ragionevoli aspettative della persona da valutarsi con riferimento al rapporto tra quest'ultima e il titolare [84]. Il legittimo interesse quale condizione di liceità del trattamento, pertanto, presuppone un rapporto già in essere tra il titolare e la persona interessata, rapporto che, nel caso dei servizi di pagamento, si instaura nel momento in cui l'utente si avvale dell'attività di un TPP o del proprio PSP, ed è lecito solo al contestuale ricorrere delle condizioni sopra indicate [85].

iii) L'ultima situazione si presenta nel caso in cui i TPP trattano i dati dell'utente per finalità diverse da quelle strettamente connesse all'esecuzione del servizio di pagamento, come ad esempio a fini di profilazione [86] e di *marketing*. Questa circostanza è probabilmente quella più delicata in relazione ai dubbi posti dalla dottrina [87] circa il rapporto e il coordinamento tra la normativa specifica della PSD2 e quella generale del GDPR. Infatti, la possibilità di

[84] Il rapporto in essere tra il titolare e l'interessato segna, quindi, i confini delle finalità che possono essere perseguite dal titolare con il trattamento, visto che è dalla natura e dalle caratteristiche del rapporto stesso che l'interessato può desumere come e in che termini i suoi dati personali saranno utilizzati. Pertanto, il paziente di un ospedale potrà ragionevolmente aspettarsi che l'ospedale tratterà i dati relativi al suo stato di salute, ma non che il trattamento includa i dati personali relativi alla sua situazione finanziaria. Il tema è, quindi, particolarmente delicato ed importante in quanto richiede un'attenta disamina da parte del titolare del suo concreto rapporto con l'interessato per evitare che il trattamento dei dati diventi illegittimo.

[85] Si deve sottolineare che per quanto riguarda la base giuridica del legittimo interesse del titolare – che permette di eseguire il trattamento senza il preventivo consenso dell'interessato – il rapporto intercorrente tra le due parti non rileva solamente per l'interessato, ma è un parametro per valutare *ex post* la liceità della condotta del titolare e verificare se il trattamento che ha eseguito è conforme a ciò che l'interessato poteva immaginare. Il rapporto tra titolare e interessato, pertanto, diventa elemento di riferimento per l'interessato e limite all'attività del titolare.

[86] Il GDPR considera profilazione «*qualsiasi forma di trattamento di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*» (art. 4, par. 1, n. 4). Si ha, quindi, profilazione in presenza di un trattamento automatizzato di dati personali eseguito al fine di valutare alcuni aspetti personali di una persona fisica.

[87] Cfr. M. RABITTI, A. SCIARRONE ALIBRANDI, (nt. 14), 54 ss., in cui viene evidenziato che il favore della Direttiva PSD2 per il fenomeno dell'*open banking* – inteso come condivisione di dati tra gli intermediari – ha un impatto sui dati personali degli utenti, sia sotto il profilo della sicurezza sia sotto quella della profilazione della clientela per le più disparate finalità, che non può essere trascurato, soprattutto se si tiene conto del fatto che ormai le banche sono minacciate da colossi del *web* in grado di offrire numerosi e innovativi servizi su misura del cliente.

tale trattamento sembrerebbe categoricamente esclusa dalla PSD2 ma, stante il richiamo in essa contenuto (art. 94, par. 1) alla normativa sul trattamento dei dati personali e, quindi, oggi al GDPR, è a quest'ultima che si deve far riferimento per verificare se le attività di profilazione e di *marketing* da parte degli intermediari debbano essere considerate del tutto vietate o se lecite, seppure a determinate condizioni.

In proposito, occorrono alcune precisazioni. Per quanto riguarda la profilazione, il GDPR affronta direttamente il tema e prevede un generale divieto di sottoporre i dati personali di una persona fisica al cosiddetto trattamento automatizzato - cioè quello effettuato solo attraverso l'uso di sistemi tecnologici e senza alcun intervento umano - quando sulla base di tale attività venga presa un decisione che produce effetti giuridici o incide significativamente sull'interessato (art. 22, par. 1). Tuttavia, sono previste delle eccezioni riguardanti i casi in cui: la decisione è necessaria per la conclusione o l'esecuzione di un contratto tra il titolare e l'interessato [par. 2, lett. a)]; il trattamento è previsto dalla legge (par. 2, lett. b); vi è stato l'esplicito consenso dell'interessato [par., 2, lett. c)].

Relativamente al *marketing,* invece, la questione è più complessa dato che mancano disposizioni specifiche e l'unico riferimento diretto a tale attività si riscontra nel Considerando n. 47 del GDPR secondo il quale il trattamento per finalità di *marketing* diretto, ovvero quello senza intermediazione tra venditore e titolare, può essere considerato legittimo interesse di quest'ultimo. Da tale affermazione si dovrebbe desumere che il trattamento finalizzato all'esecuzione di *marketing* diretto è, in linea di principio, lecito in forza della lett. f), par. 2, art. 6, GDPR, e, di conseguenza, potrebbe essere effettuato senza il previo consenso dell'interessato purché con tale trattamento non vengano pregiudicati i suoi diritti e le sue libertà fondamentali. Tuttavia, nonostante ai Considerando sia stata attribuita una valenza interpretativa particolarmente rilevante [88], il riferimento riportato non può essere considerato decisivo. Infatti, bisogna ricordare che l'art. 13 della Direttiva (Ce) 2002/98 (Direttiva *e-privacy* relativa al trattamento dei dati personali nel settore delle comunicazioni elettroniche) pone dei limiti alle comunicazioni a fini di commercializzazione diretta

[88] Cfr. V. CUFFARO, (nt. 51), 3 ss. il quale sottolinea come la nuova disciplina sul trattamento dei dati personali assegni ai considerando una peculiare funzione interpretativa -- circostanza evidenziata dal cospicuo numero di considerando che precedono le norme del Regolamento e dal fatto che essi sono più ricchi di contenuti – in quanto è grazie ad essi che si può cogliere il cambiamento di *ratio* avvenuto con il GDPR. Infatti, quest'ultimo rende esplicita l'attuale esigenza, dovuta soprattutto alla pervasività della tecnologia informatica, di bilanciare gli interessi coinvolti dal trattamento dei dati personali e il trattamento stesso (12).

vietando l'uso di sistemi automatizzati in assenza di un preliminare consenso dell'interessato a ricevere tali tipi di comunicazione (par. 1) e permettendo l'utilizzo delle coordinate elettroniche solamente in ordine alla commercializzazione dei servizi propri del titolare del trattamento e a patto che all'utente sia offerta, in modo chiaro e distinto, la possibilità ad opporvisi (par. 2). Le disposizioni citate, sebbene limitate al caso delle comunicazioni elettroniche, hanno come conseguenza una limitazione dell'attività del titolare del trattamento che voglia perseguire finalità di *marketing* diretto; infatti, dalla loro applicazione deriva che il trattamento dei dati personali del cliente deve essere circoscritto alle comunicazioni tramite posta elettronica e alla commercializzazione di prodotti o servizi del titolare, analoghi a quelli già acquistati dall'interessato; in ogni caso, sul titolare gravano precisi obblighi informativi, soprattutto, per ciò che riguarda il diritto d'opposizione dell'interessato (art. 21, GDPR).

In sintesi, coordinando le disposizioni della PSD2 con quelle del GDPR, si deve ritenere che ai TPP e ai PSP è concesso trattare i dati dei propri utenti per fini diversi da quelli strettamente connessi alla loro attività di prestazione del servizio di pagamento. Tuttavia, ad eccezione dei casi di prevenzione delle frodi – in cui il consenso non è richiesto – e della commercializzazione diretta nei limiti posti dalla Direttiva *e-privacy*, il consenso dell'utente/interessato è sempre necessario [89].

[89] Il consenso, base giuridica ai sensi dell'art. 6, par. 1, lett. a), GDPR, deve consistere in una manifestazione di volontà libera, specifica ed inequivocabile (cfr. Considerando n. 32) e deve possedere i requisiti previsti dall'art. 7, GDPR. Le disposizioni di tale articolo, infatti, sono particolarmente importanti per ciò che riguarda la tutela dell'interessato in quanto impongono specifici obblighi al titolare che si avvalga di tale base giuridica per eseguire il trattamento. In particolare, sul titolare grava, innanzitutto, un obbligo di informazione, il cui contenuto è specificato negli artt. 12, 13 e 14 GDPR, informazione che deve essere fornita in maniera comprensibile e facilmente accessibile se il consenso dell'interessato è prestato all'interno di una dichiarazione relativa ad altre questioni (art. 7, par. 2). Inoltre, al titolare è espressamente vietato di porre in essere condotte scorrette tese a far dipendere l'esecuzione di un contratto o di un servizio dal rilascio del consenso al trattamento per fini ulteriori (art. 7, par. 4). Infine, egli deve essere in grado di dimostrare che l'interessato ha rilasciato il proprio consenso al trattamento dei dati personali (art. 7, par. 1). In relazione a quest'ultimo punto, particolarmente importante ai fini della valutazione della liceità della condotta del titolare, si deve sottolineare che, a differenza dell'informazione che deve essere fornita all'interessato in forma scritta per assicurarne la conoscibilità in concreto, il GDPR non prevede requisiti di forma per la manifestazione del consenso dell'interessato; tuttavia il Considerando n. 32 del GDPR fornisce alcune indicazioni per quanto riguarda la manifestazione del consenso anche mediante mezzi elettronici, tema su cui sono sorte numerose questioni soprattutto in ordine all'effettiva chiarezza e comprensibilità dei mezzi attraverso i quali il consumatore dovrebbe manifestare il consenso

Per concludere il tema relativo al trattamento dei dati dell'utente, occorre fare un riferimento anche al trattamento dei suoi dati biometrici di cui gli intermediari possono venire a conoscenza quando essi siano utilizzati anche come credenziali personalizzate dell'utente stesso.

Come già evidenziato, i dati biometrici sono oggetto della disciplina settoriale, in quanto possono essere utilizzati dal sistema di sicurezza predisposto dall'intermediario, e dalla disciplina generale, in quanto appartengono ad una categoria ritenuta dal legislatore bisognosa di particolare tutela, in considerazione dei profili della persona fisica coinvolti e dei pregiudizi che un trattamento illecito potrebbe arrecare ai diritti e alle libertà fondamentali dell'individuo.

In relazione a ciò, la dottrina [90] ha rilevato l'incongruenza tra la definizione

all'utilizzo dei suoi dati personali. Per un approfondimento in argomento, cfr. F. CAGGIA, *Libertà ed espressione del consenso*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, Giappichelli, 2020, 249 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, 113 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Le riforme del diritto italiano*, diretto da G. FINOCCHIARO, Bologna, Zanichelli, 2017, 101 ss.; A. MANTELERO, *Responsabilità e rischio nel Reg. Ue 679/2016*, in *Nuove leggi civ. comm.*, 2017, 144 ss.; F. PIZZETTI, (nt. 7), 44 ss. Il consenso è uno degli elementi a cui il legislatore comunitario è ricorso spesso, soprattutto, in ordine a quei casi in cui la manifestazione della volontà dell'individuo è ritenuta elemento irrinunciabile dal legislatore. Con particolare riferimento alla rilevanza del consenso nelle relazioni via internet, v. G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss.. Sia la disciplina specifica sui servizi di pagamento sia quella sul trattamento dei dati personali valorizzano la funzione del consenso in quanto espressione del potere di autodeterminazione dell'individuo. In relazione alla disciplina sul trattamento dei dati personali, tuttavia, è stato osservato – ma la riflessione vale per tutti i casi di utilizzazione dei servizi della rete internet – che spesso il consenso, inteso come atto di volontà grazie al quale un soggetto esercita il proprio potere di decidere liberamente sulle questioni che lo riguardano, non garantisce un'effettiva ed efficace tutela al soggetto che lo esprime ma si riduce ad un "atto di vuota cerimonia" in quanto "come la prassi facilmente evidenzia, la lettura dell'informativa (privacy) e l'eventuale consenso prestato tendono ad essere solo un passaggio (aggiuntivo e spesso fastidioso) rispetto all'ottenimento del bene o servizio cui il trattamento dei dati personali è funzionale" (cosi I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, reperibile in internet al seguente indirizzo: http://www.dimt.it).

[90] M. RABITTI, A. SCIARRONE ALIBRANDI, (nt. 14), 57, dove osservano che i dati sensibili relativi ai pagamenti non sono gli stessi dati che il GDPR considera dati sensibili e per i quali è prevista una tutela più forte; tale divergenza definitoria avrebbe come immediata conseguenza una più difficile individuazione della normativa applicabile nel caso in cui l'intermediario sia a conoscenza di tali tipi di dati.

di dati sensibili contenuta nella PSD2 e quella generale del GDPR. Tuttavia, le discipline sul trattamento di tali dati non sono inconciliabili ed è, quindi, possibile prospettare l'applicazione di entrambe. Infatti, il quadro che si delinea è il seguente.

In linea generale, si deve ritenere che - in assenza di qualsiasi riferimento nella PSD2 al trattamento dei dati biometrici da parte degli intermediari (sia PSP di radicamento del conto sia TPP) – siano applicabili le disposizioni dell'art. 9 del GDPR e, in particolare, quella contenuta nel par. 2, lett. a) che consente il loro trattamento dietro esplicito consenso dell'utente e per finalità specifiche. L'intermediario può, perciò, trattare i dati biometrici dell'utente a patto che questi lo abbia espressamente autorizzato e che il trattamento sia finalizzato all'esecuzione dell'attività di prestazione del servizio richiesto.

Inoltre, se i dati biometrici sono utilizzati come credenziali personalizzate dell'utente, rientrano anche nella categoria dei dati sensibili relativi ai pagamenti, categoria prevista dalla PSD2 che sottopone il loro utilizzo da parte dei TPP ad ulteriori e più stringenti regole; infatti, gli artt. 66, par. 2, lett. e) e 67, par. 2, lett. e) della PSD2 vietano rispettivamente al PISP di conservarli e agli AISP di chiedere i dati sensibili relativi ai pagamenti che siano collegati ai conti di pagamento. Questa maggiore tutela dell'utente si spiega con il fatto che quest'ultimo non ha un rapporto continuativo con i TPP i quali, peraltro, svolgono un'attività per l'esecuzione della quale non sempre è necessario il trattamento di tali dati [91].

7. *Il trattamento dei dati personali del beneficiario.*

Un ultimo aspetto che merita attenzione riguarda la posizione del beneficiario di un pagamento eseguito tramite servizi elettronici. Infatti, un'operazione, sia che venga eseguita direttamente tramite PSP di radicamento del conto sia che venga posta in essere tramite PISP, ha come indispensabile presupposto che i dati del beneficiario vengano comunicati dal pagatore al proprio intermediario o al PISP. In proposito, si ricorda che l'intermediario del pagatore non ha alcun rapporto giuridico o fattuale con il beneficiario del pagamento; questi, di conseguenza, pur essendo parte dell'operazione, non autorizza esplicitamente l'intermediario del pagatore a trattare i suoi dati e non può

[91] Ad esempio, quando si utilizza il servizio di *Paypal* tramite l'*App* scaricata sull'*iPhone*, l'utente può decidere se eseguire l'accesso tramite l'inserimento della *password* o tramite il riconoscimento dell'impronta digitale; solamente nel secondo caso, vi è un utilizzo dei suoi dati biometrici.

esercitare un controllo diretto sul trattamento eventualmente eseguito. Ciò ha posto la questione del trattamento dei dati del beneficiario, la cosiddetta "parte silente", da parte dell'intermediario del pagatore e delle norme applicabili.

Sul punto la PSD2 non prende alcuna posizione e le uniche disposizioni che possono essere utili all'interprete per ricostruire la disciplina sono quelle riguardanti l'obbligo dell'intermediario del beneficiario di fornire al proprio cliente, subito dopo l'esecuzione di un'operazione, un rapporto che gli permetta di individuare, ove opportuno, tutte le informazioni che sono state trasmesse con l'operazione stessa [artt. 49, par. 1, lett. a) e art. 58, par. 1, lett. a), PSD2]. Così il beneficiario avrà la possibilità di conoscere quali sono i dati personali che gli intermediari si sono scambiati per eseguire l'operazione.

Per quanto riguarda il GDPR, un'utile indicazione circa le disposizioni applicabili si riscontra nella lettera del 5 luglio 2018 con la quale l'EDPB [92] individua la condizione di liceità – cioè la base giuridica che legittima il trattamento dei dati del beneficiario [art. 6, par. 1, lett. f), GDPR] - nell'interesse legittimo del titolare (ovvero l'intermediario del pagatore) a poter eseguire la prestazione dedotta nel contratto stipulato con il pagatore.

Inoltre, l'EDPB si preoccupa di specificare che, in linea generale, tutti i trattamenti devono essere eseguiti tenendo sempre presenti i principi di minimizzazione, limitazione e trasparenza, che sono principi cardine del GDPR (art. 5). Tali principi, nel contesto dei pagamenti elettronici, trovano applicazione nel fatto che il trattamento dei dati del beneficiario deve essere limitato all'esecuzione dell'operazione di pagamento, elemento che determina non solo le finalità per cui i dati vengono raccolti dall'intermediario del pagatore, ma anche le legittime aspettative del beneficiario che, consapevole del pagamento eseguito dal pagatore, potrà facilmente dedurre che alcuni dei suoi dati personali saranno utilizzati per poter portare a termine il procedimento di pagamento.

Tale soluzione, sempre ad avviso dell'EDPB, è confermata dalla disciplina specifica sui servizi di pagamento PSD2 che, relativamente agli obblighi gravanti sui TPP, vieta espressamente l'utilizzo, la conservazione e l'accesso a dati per fini diversi dalla prestazione dello specifico servizio richiesto dall'utente [art. 66, par. 3, lett. g) e art. 67, par. 2, lett. f), PSD2].

In sintesi, il trattamento dei dati personali del beneficiario da parte del PSP o del TPP del pagatore deve ritenersi, in linea di principio, consentito; in particolare, dal combinato disposto delle norme del GDPR e della PSD2 si ricava, da un lato, che l'operazione di pagamento è circostanza sufficiente a giustifi-

[92] Vedi nota 81.

care il trattamento, nonostante tra l'intermediario del pagatore e il beneficiario/interessato non vi sia alcun rapporto diretto, d'altro lato, che quest'ultimo è tutelato tramite la delimitazione dell'area di legittimità del trattamento al solo utilizzo che egli potrebbe ragionevolmente aspettarsi.

In questa conclusione si trova il punto di equilibrio tra la necessità dell'intermediario del pagatore di poter eseguire la propria prestazione senza dover chiedere al beneficiario il preventivo consenso al trattamento dei suoi dati e il diritto di quest'ultimo a poter controllare l'utilizzo che ne viene fatto. Infatti, da una parte le norme generali del GDPR si preoccupano di impedire che l'intermediario venga gravato da oneri che inficerebbero l'efficienza e la rapidità dell'operazione richiesta, dall'altra, le norme specifiche della PSD2 permettono di individuare i limiti concreti posti all'attività di trattamento, impedendo così che gli intermediari e, in particolare i TPP, possano porre in essere condotte scorrette, tese ad aggirare le regole in tema di consenso fissate dal GDPR e ad utilizzare i dati personali del beneficiario per finalità diverse da quelle strettamente connesse all'esecuzione della loro attività.