Maddalena Rabitti

Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento

Sommario: 1.Il problema – 2. Il riparto di competenze tra *Authorities* e la giurisprudenza – 3. Banca d'Italia e AGCM: *Credit Surcharge* e pratiche commerciali scorrette. Una buona risposta normativa – 4. Un nuovo problema. Il rapporto tra PSD2 e GDPR – 5. Gli strumenti di tutela: il consenso – 6. (*Segue*). L'*accountability* – 7. Conclusioni: verso una competenza concorrente tra *Authorities.*

1. *Il problema*

La normativa sui servizi di pagamento[1] è un esempio paradigmatico di una disciplina di settore che finisce per essere crocevia di interessi diversi che, in concreto, pongono rilevanti problemi di bilanciamento. L'analisi di impatto del d.lgs. 218/17 mostra la difficoltà che la *compliance* a questa disciplina comporta, tanto più che si aggiungono i provvedimenti di Banca d'Italia che sono necessari per rendere effettiva l'attuazione della PSD2 e anche i *Regulatory Tecnical Standards* EBA entreranno in vigore nel settembre 2019.

Obiettivo dichiarato della PSD2 è quello di garantire una maggiore efficienza, concorrenza e trasparenza nell'offerta di servizi di pagamento rafforzando, al contempo, la fiducia dei consumatori in un mercato dei pagamenti armonizzato[2]. Tra gli ulteriori obiettivi strumentali (anche

[1] Introdotta con la Direttiva PSD2, attuata con d.lgs. 18/2017, che ha modificato il d.lgs. 11/10.

[2] 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. Comm.*, 2018, p. 839 ss.; S. Balsamo Tagnani, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2,* in *Contratto e impresa Europa,* 2018, p. 609 ss. Nelle more della pubblicazione di questo articolo, molti altri contributi hanno visto la luce. Per una sintesi dei problemi principali si rinvia a Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento tra PSD2, criptovalute e rivoluzione digitale*, a cura di F. Maimeri e M. Mancini, in *Quad. Giur. 87/2019*. Si rinvia anche a M. Rabitti - A. Sciarrone Alibrandi, *I servizi di*

impliciti) perseguiti, primario è quello di creare un *Common Level Play Field* per i fornitori di servizi di pagamento e adeguate tutele per gli utenti. Su tutto, poi, si pone l'interesse del sistema finanziario europeo a consentire, in chiave pro-concorrenziale, l'ingresso a nuove categorie di prestatori di servizi di pagamento (cosiddetti *Third parties providers:* TPP) che si aggiungono a quelli già autorizzati a operare nel settore dei servizi di pagamento tramite internet.

Sul punto, la PSD2 (e il d.lgs. 218/2017 che la attua) innova fortemente la disciplina sui servizi di pagamento, prevedendo due nuove categorie di operatori non finanziari: coloro che effettuano "servizio di disposizione di ordini di pagamento" (PISP: *Payment Initiation Service Providers*)[3] e coloro che svolgono un "servizio di informazione sui conti" (AISP: *Account Information Service Provider*)[4].

Il legislatore risponde così alle crescenti richieste della clientela di potersi avvalere di forme di pagamento nuove e più evolute, che sono richieste soprattutto dalle imprese che operano attraverso piattaforme digitali di servizi e prodotti (*e-commerce*). Le APIs[5] e il principio di *net neutrality* sono gli strumenti prescelti per favorire l'operatività dell'*Open Banking*.

Si realizza così un complessivo regime di favore per chi voglia avvalersi degli strumenti di pagamento, che si sostanzia: in maggiori opportunità di scelta nei servizi di pagamento; in una semplificazione dell'onere della prova a favore del cliente per l'ipotesi di utilizzo fraudolento degli strumenti di pagamento; in limitazioni a spese e commissioni e nel divieto di *credit surcharge,* solo per elencare alcune tra le misure introdotte.

Tuttavia, l'interprete deve valutare l'impatto della nuova disciplina

pagamento su PSD2 e GDPR: Open banking e conseguenze per la clientela, in *Liber Amicorum Guido Alpa*, a cura di F. Capriglione, Cedam, Padova 2019, p. 711 ss.

[3] Esso ha per oggetto 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.

[4] Si occupa di fornire un servizio *online* avente ad oggetto informazioni relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore o presso più prestatori di servizi di pagamento. Si veda art. 2, comma 1, lett. b-*bis)* e lett. b- *ter*) del d.lgs. 218/2017.

[5] *Application Programming Interfaces,* sono costituiti da un insieme di protocolli che definiscono in che modo posso interagire le componenti dei *software*. A livello europeo, il Piano d'Azione della Commissione ha previsto lo sviluppo, da parte di imprese e fornitori di nuove tecnologie, di interfacce di programmazione delle applicazioni (API) standardizzate e conformi a PSD2 e GDPR, alle quali gli altri operatori saranno tenuti ad adattarsi. L'obbiettivo è quello di giungere a una standardizzazione delle modalità di esecuzione dei pagamenti digitali e di rendere più sicure le transazioni, ottenendo così una maggior tutela dei consumatori.

anche da punti di vista diversi: se è vero, ad esempio, che occorre agevolare e semplificare i pagamenti anche *online*, non si può trascurare il rischio che un eccesso di liberismo metta a repentaglio la sicurezza dei dati personali degli utenti, con quel che ne consegue sotto il profilo sia della profilazione della clientela, sia della stabilità del sistema bancario, che potrebbe prossimamente subire un attacco concorrenziale dai giganti del *web* in grado di offrire i più disparati servizi "su misura" del cliente[6].

Questo rischio, tutt'altro che remoto, suscita una serie di perplessità sulla possibilità concreta di attuare la PSD2 senza prima risolvere alcune questioni cruciali per la tutela dei clienti, ma anche per la sopravvivenza del sistema bancario così come è oggi.

Il punto che si intende approfondire in questa sede è quello del riparto di competenze tra Autorità amministrative indipendenti sui due dei profili ora menzionati: il divieto di *credit surcharge* e l'accesso ai dati da parti delle *Third Parties Provider*. La scelta di questo duplice angolo prospettico si giustifica con l'idea di svolgere alcune riflessioni di sistema sul rapporto tra la PSD2, che è disciplina settoriale e verticale e le discipline generali e orizzontali che incrocia, quali il Codice del Consumo e il recente Regolamento GDPR. Come si è recentemente affermato, "agli incroci con i silos verticali non ci sono semafori ma rotonde; si tratta di condividere regole minime di competenze o principi, sufficienti per superare i contrasti tra la tutela dei dati e promozione della concorrenza nel settore bancario (PSD2)"[7].

2. *Il riparto di competenze tra* Authorities *e la giurisprudenza*

Il riparto di competenze tra *Authorities* è un problema ormai classico che, anziché trovare una soluzione nel tempo, ha assunto progressiva complessità e stenta a trovare una risposta di sistema. Le ragioni che possono addursi per spiegare questa difficoltà sono molte.

In primo luogo, è frequente che si assista ad un fenomeno di *overlapping* tra norme che talvolta disciplinano un medesimo fatto in modo diverso.

[6] F. Bassan, *Potere dell'algoritmo e resistenza dei mercati*, Rubbettino, 2019, p. 40 ss. mette in guardia sul rischio che in ambito bancario, assicurativo e finanziario la capacità di gestire dati acquisterà nel prossimo futuro rilievo decisivo, perché sono comparti in cui i bassi investimenti tecnologici, la scarsa condivisione di informazioni e l'assenza di standard tecnologici condivisi e avanzati evidenziano la resilienza minima del sistema attuale in caso di concorrenza aggressiva ad opera di *newcomers* esperti in gestione dati.

[7] Ancora, F. Bassan, *op. cit.,* p. 42.

Capita, cioè, che una disciplina settoriale si intersechi (sovrapponga) con altre discipline – che a volte tutelano lo stesso interesse (ponendosi perciò il problema solo in termini di intensità della tutela) a volte, invece, tutelano interessi diversi – con la conseguenza di dovere stabilire come gestire l'*overlapping* e quali siano le Autorità competenti[8].

L'esempio ad oggi più eclatante, come si dirà, è quello delle pratiche commerciali scorrette, ma non solo. L'ultimo dibattito investe persino la possibilità di immaginare, in prospettiva e allo stato in modo provocatorio, la possibilità di unificare le due autorità dell'AGCOM e della Privacy, perché i principali problemi in tema *privacy* sono legati all'uso dei dati personali su *devices* mobili, app e *web*, ragion per cui la competenza anche dell'AGCOM diventa innegabile e decisiva[9]. Ipotesi alternative, meno radicali, presuppongono comunque una collaborazione più strutturata tra AGCOM e Garante Privacy.

Una seconda ragione che spiega la complessità della questione si può individuare nella matrice europea della maggior parte delle normative che introducono nuove regole del mercato. Accade, cioè, che le norme europee – specialmente i regolamenti e le Direttive *self executing* – entrino direttamente a fare parte dell'ordinamento nazionale comportando un necessario adeguamento del sistema di regole già tendenzialmente completo dello Stato membro che le accoglie. Così, ad esempio, nel tempo si è progressivamente ampliato l'ambito di operatività dell'Autorità garante della concorrenza e del mercato (AGCM), che ha assunto su di sé competenze che

[8] Si pensi alla materia del *market abuse* e, più in generale, al tema del *ne bis in idem*, su cui si sono succeduti interventi della CEDU, della Corte di Giustizia e della Corte Costituzionale e di Cassazione. Per un approfondimento dell'evoluzione giurisprudenziale, si veda Assonime, Ne bis in idem *e potestà sanzionatoria di Banca d'Italia e Consob nella giurisprudenza dell'ultimo quinquennio*, il Caso 1/2019. Sul *coté* sostanziale e sui piani mobili di tutela, cfr. A. Zoppini, *Sul rapporto di specialità tra norme appartenenti ai "codici di settore". Lo* ius variandi *nei codici del consumo e delle comunicazioni elettroniche*, in *Riv. dir. civ.*, 2016, p. 136.

[9] È questa l'opinione di A. Nicita, espressa durante una conferenza dell'Università di Napoli il 23 gennaio 2019 il quale ha dichiarato che: "Sarebbe auspicabile una fusione di Agcom e Garante per la privacy, le cui competenze, sancite a livello europeo, resterebbero intatte e costituirebbero un importante tassello nel percorso per la costruzione di un mercato regolato dell'uso del dato, che va affidata al legislatore. Man mano che il dato diventa il prodotto al centro dei modelli di business della comunicazione digitale, il campo regolatorio dell'Autorità per le garanzie nelle comunicazioni e quello del Garante per la protezione dei dati personali appaiono sempre più sovrapponibili". "Il proliferare di competenze diverse ad *authority* distinte non è certo d'aiuto" ha continuato: "non solo perché possono sempre manifestarsi obiettivi diversi tra le varie autorità indipendenti, ma soprattutto perché questi obiettivi potrebbero essere segmentati o addirittura confliggenti".

originariamente non le erano attribuite in quanto non strettamente legate alla materia della concorrenza.

In altri termini, l'ingresso di una nuova normativa di tutela del mercato può rendere necessario individuare l'autorità amministrativa indipendente competente a vigilare su quel mercato di riferimento, con la necessità per il legislatore di ripensare le attribuzioni delle *Authorities* già esistenti e di rimettere in discussione il criterio funzionale che il legislatore ha seguito al momento dell'istituzione di ciascuna.

Queste ragioni, pur non esaustive, sono sufficienti a rivelare un quadro incerto e mutevole sotto il profilo regolatorio. A fronte dell'inadeguatezza del legislatore, la risposta di sistema ha provato a darla la giurisprudenza che, sempre più, tende a occupare gli spazi lasciati vuoti dalla legge concorrendo alla progressiva "giurisdizionalizzazione" del diritto, con cui si amplia la sfera di discrezionalità del giudice chiamato a partecipare direttamente alla creazione della regola del caso concreto[10]. Anche in questo caso vale, perciò, la pena richiamare la giurisprudenza che si è pronunciata sul tema.

La vicenda è nota e riguarda la competenza sulle pratiche commerciali scorrette in materia di comunicazioni elettroniche: si trattava di stabilire se all'accertamento e sanzione della pratica commerciale scorretta fosse tenuta l'AGCM o l'AGCOM. Rileva, sul piano delle fonti applicabili, l'art. 4, comma 3, della Direttiva 2005/29 CE in materia di pratiche commerciali scorrette secondo cui: "In caso di contrasto, le disposizioni contenute in direttive o in altre disposizioni comunitarie e nelle relative norme nazionali di recepimento che disciplinano aspetti specifici delle pratiche commerciali scorrette prevalgono sulle disposizioni del presente titolo e si applicano a tali aspetti specifici". Questa disposizione è stata sostanzialmente trascritta dall'art. 19, comma 3, del Codice del Consumo. Con Adunanza plenaria del 2012 il Consiglio di Stato ha affermato che il complesso di regole *ex* art. 19,

[10] Si delinea così una nuova fisionomia del ruolo del giudice, specie se di grado superiore, che è interprete del diritto, ma che è anche tenuto a integrare le regole con funzione nomofilattica, con l'obiettivo di dare uniformità e certezza. È questa, ormai, un'esigenza fortemente avvertita che trova la propria origine nel rapporto tra crisi della regolazione e esigenza dell'esecuzione del diritto. Per un approfondimento, si rinvia a quanto già scritto in M. Rabitti, *Il ruolo della Corte di giustizia nel diritto dell'economia*, in *Giudicare l'economia, AGE*, 2/2018, p. 347 ss. e in *La Corte di Giustizia tra scelte di mercato e interessi protetti,* in *I Giudici e l'economia*, a cura di L. Ammannati, P. Corrias, F. Sartori, A. Sciarrone Alibrandi, Torino 2018, p. 459 ss.; M.R. Damaška, *I volti della giustizia e del potere. Analisi comparatistica del processo,* trad. it., Bologna 1991, p. 30 ss., e p. 270 ss.; A.A.S. Zuckermann, *Court Control and Party Compliance. The Quest for Effective Litigation Management*, in *The Reforms of Civil Procedure in Comparative Perspective*, a cura di N. Trocker e V. Varano, Torino 2005, p. 143 ss.; *Il giudice e la legge*, numero monografico di *Questione giustizia*, 2016.

comma 3, "si iscrive nell'ambito del principio di specialità" tra fattispecie normative, ponendo così una limitazione generale all'operatività della disciplina delle pratiche commerciali scorrette e, dunque, alla competenza dell'AGCM, in presenza di una disciplina settoriale esaustiva[11].

Tuttavia, con le sentenze del 9 febbraio 2016, il Consiglio di Stato, in Adunanza plenaria[12], adito sul punto del riparto di competenze, ha mutato indirizzo, concludendo nel senso di riconoscere all'AGCM la competenza a irrogare le sanzioni per "pratica commerciale considerata in ogni caso aggressiva", anche se in materia settoriale di competenza di altra Autorità. Si è, cioè, ritenuto che là dove una condotta, pur comportando la violazione di obblighi informativi dettati da una disciplina settoriale, integri una pratica connotata da profili di aggressività, si applicano le disposizioni del Codice del Consumo e, dunque, è legittimata all'azione l'AGCM, con i poteri di cui all'art. 27 del Codice del Consumo. Il ragionamento condotto dal Consiglio di Stato muove da un'idea diversa del criterio di specialità in relazione all'art. 3, paragrafo 4, della Direttiva 2005/29/CE, che viene definito "per progressione di condotte lesive": ciò significa non fare valere davvero di per sé la specialità per fattispecie normative, quanto piuttosto fare prevalere l'illecito di maggiore gravità, con conseguente applicazione della sanzione più afflittiva. Non è stato questo, tuttavia, l'epilogo della vicenda giurisprudenziale. Lo stesso Consiglio di Stato (Sezione VI) ha ritenuto di non potersi adeguare al principio di specialità per progressione di condotte lesive se non dopo avere sollevato una serie di quesiti di interpretazione pregiudiziale alla Corte di Giustizia sulla compatibilità tra la Direttiva 2005/29/CE e le norme di attuazione del Codice del Consumo[13].

[11] Il Tar Lazio, nelle sentenze nn. 1742/2013 e 1754/2013, in linea con il Consiglio di Stato, ha ribadito l'inapplicabilità della disciplina (generale per materia) sulle pratiche commerciali in presenza di una disciplina specifica (settoriale) idonea a ricomprendere la condotta contestata all'operatore e la cui repressione è affidata a uno specifico soggetto pubblico dotato di poteri ispettivi e sanzionatori. La convivenza tra Autorità indipendenti trasversali, istituite a tutela di specifici interessi pubblici di portata generali, e Autorità di settore, preposte in via esclusiva ad uno specifico settore economico, ha sempre dato luogo a interferenze tra le rispettive attribuzioni. Sul punto si veda S. Cassese, *L'Autorità garante della concorrenza e del mercato nel "sistema" delle autorità indipendenti*, in *Giorn. dir. amm.*, 2011, p. 1.

[12] Chiamato a pronunciarsi di nuovo anche a seguito della procedura di infrazione del 2013 ad opera della Commissione Europea.

[13] Per approfondimenti sulla questione e sull'excursus giurisprudenziale vedi M. Bertani, *Pratiche commerciali scorrette e violazione della regolazione settoriale tra concorso apparente di norme e concorso formale di illeciti*, in *Nuove Leggi Civ. Comm.*, 2018, p. 926 ss.; V. Mosca, *Il riparto di competenze sulla tutela del consumatore all'esame della Corte di Giustizia*, in *Giorn. dir. amm.*, 2017, p. 519 ss.; M.S. Bonomi, *Tutela del consumatore, pratiche commerciali scorrette e riparto di competenze tra autorità indipendenti*, in *Giorn. dir. amm.*, 2016,

Due i profili che qui rilevano: (i) se il principio di specialità debba essere inteso come principio regolatore nei rapporti tra ordinamenti o tra norme o tra *Authorities*; (ii) se la nozione di contrasto presupponga una vera e propria "antinomia" tra le disposizioni o se sia sufficiente che norme settoriali diverse dettino discipline difformi in relazione alla specificità del settore[14].

La Corte di Giustizia si è pronunciata con la sentenza del 13 settembre 2018 chiarendo che, qualora ci sia normativa europea in potenziale conflitto con normativa di matrice non europea, prevale la prima e che la Direttiva sulle pratiche commerciali scorrette si applica solo se non esistono specifiche norme del diritto dell'Unione che disciplinino altrimenti aspetti specifici delle condotte che integrano la pratica scorretta[15]. Da ciò la Corte trae alcune importanti conseguenze: un problema di riparto di competenze tra *Authorities* può porsi solo laddove sussista un "contrasto" tra le disposizioni applicabili, che si ravvisa però solo quando: "il rapporto tra due disposizioni va oltre la mera difformità o la semplice differenza, mostrando una divergenza che non può essere superata mediante una formula inclusiva che permetta la coesistenza di entrambe le realtà, senza che sia necessario snaturarle".

p. 793 ss.

[14] Il Consiglio di Stato all'atto della definizione del merito deferiva alla Corte di Giustizia due gruppi di quesiti. Il primo gruppo riguardava, in estrema sintesi, gli artt. 8 e 9 della Direttiva 2005/29/Ce e l'allegato 1 di detta Direttiva (concernenti le singole ipotesi di pratiche commerciali scorrette); il secondo gruppo aveva, invece, ad oggetto la *ratio* della Direttiva generale 2005/29/Ce, nonché il principio di specialità di cui all'art. 3, comma, 4 della stessa (i rapporti tra discipline). Più in particolare, con le questioni prima e seconda, il giudice del rinvio chiedeva se la nozione di "pratica commerciale aggressiva", di cui agli artt. 8 e 9 della Direttiva 2005/29, o la nozione di "fornitura non richiesta", ai sensi dell'allegato I, punto 29, di tale Direttiva, debba essere interpretata nel senso che ricomprende condotte consistenti nella commercializzazione, da parte di un operatore di telecomunicazioni, di carte SIM sulle quali sono preimpostati e preattivati determinati servizi, quali la navigazione Internet e la segreteria telefonica, senza che il consumatore sia stato previamente ed adeguatamente informato né di tale preimpostazione e preattivazione né dei costi di tali servizi. Le questioni dalla terza alla sesta – quelle che rilevano ai fini del nostro tema – vertevano sostanzialmente sui rapporti tra discipline e sulla possibilità di valutare, ai sensi del richiamato art. 3, paragrafo 4, della Direttiva 2005/29, una condotta integrante una fornitura non richiesta alla luce delle disposizioni della disciplina generale sulle pratiche commerciali sleali, con conseguente incompetenza dell'Autorità di regolazione nazionale ad intervenire in applicazione della Direttiva quadro e della Direttiva servizio universale in materia di servizi di comunicazione elettronica.

[15] Corte di Giustizia, 13 settembre 2018, n. 54: "L'articolo 3, paragrafo 4, della direttiva 2005/29 dispone che, in caso di conflitto tra le disposizioni di tale direttiva e altre norme dell'Unione che disciplinano aspetti specifici delle pratiche commerciali sleali, queste altre norme prevalgono e si applicano a tali aspetti specifici. Tale direttiva trova quindi applicazione, come confermato dal suo considerando 10, soltanto qualora non esistano specifiche norme del diritto dell'Unione che disciplinino aspetti specifici delle pratiche commerciali sleali".

Al di là della soluzione del caso di specie[16], questa sentenza della Corte di Giustizia merita attenzione perché indirizza l'interprete verso una nuova configurazione dei rapporti tra autorità nei seguenti termini: la valutazione relativa alla sussistenza del contrasto riguarda solo il caso in cui uno stesso fatto è regolato da disposizioni diverse, entrambe europee, e si traduce in un conflitto reale. Se, invece, le norme riguardano il medesimo fatto, ma non si traducono in una divergenza insuperabile, magari perché sono preposte alla tutela di interessi diversi, non c'è un problema di conflitto e, dunque, possono in teoria essere applicabili entrambe le discipline e, per l'effetto, si riconosce la possibilità che più di un'Autorità amministrativa indipendente possa essere coinvolta.

Si afferma un principio tendenziale di competenze complementari di più Autorità amministrative indipendenti in chiave funzionale agli interessi protetti, salvo l'ipotesi di conflitto reale, cioè di "contrasto".

3. *Banca d'Italia e AGCM:* Credit Surcharge *e pratiche commerciali scorrette. Una buona risposta normativa*

La PSD2 attuata dal d.lgs. n. 218 del 2017 è, come si diceva, un perfetto banco di prova per testare le soluzioni da ultimo proposte dalla giurisprudenza della Corte di Giustizia in materia di "riparto di competenze tra decisori".

In linea di principio, va chiarito che l'Autorità amministrativa competente a vigilare sull'osservanza della PSD2 è la Banca d'Italia. Questa scelta può, tuttavia, essere messa in discussione almeno in due ipotesi in cui la PSD2 si sovrappone con altre discipline: il divieto di *credit surcharge* e *l'Open Banking*.

L'art. 2, comma 3, del d.lgs. 218/17 (che modifica l'art. 3, comma 4, del d.lgs. 11/10) pone il divieto di *credit surcharge* precludendo al beneficiario del pagamento di applicare commissioni o sovrapprezzi aggiuntivi ai pagatori che scelgano di avvalersi di strumenti di pagamento quali carte di debito e di credito. Questa disposizione deve, però, essere coordinata con

[16] In tal senso, nella sentenza si legge, da un lato, che la Direttiva quadro e la Direttiva servizio universale non prevedono una completa armonizzazione degli aspetti relativi alla protezione dei consumatori, dall'altro, che in base a quanto disposto dall'art. 1, paragrafo 4, della Direttiva servizio universale, l'applicabilità delle disposizioni della disciplina sulle pratiche commerciali sleali non è pregiudicata dalle disposizioni della normativa settoriale. Di qui la conclusione che non sussiste contrasto tra le disposizioni della Direttiva servizio universale e quelle della Direttiva 2005/29/CE in materia di diritto degli utenti finali.

un'analoga previsione del Codice del Consumo, che ascrive il fenomeno del *credit surcharge* tra le pratiche commerciali scorrette che possono essere oggetto di sanzione da parte dell'AGCM. Ai sensi dell'art. 21, comma 4, del Codice del Consumo si considera scorretta la pratica commerciale che richieda un sovrapprezzo di costi per il completamento di una transazione elettronica con un fornitore di beni e servizi. Inoltre, l'art. 62 del Codice del Consumo vieta ai professionisti di imporre ai consumatori spese per l'uso di questi strumenti di pagamento. Si tratta, dunque, di capire quale sia il rapporto di specialità tra queste disposizioni e quale l'Autorità chiamata a sanzionare per l'ipotesi di violazione della regola.

A soccorrere l'interprete, in questo caso, è lo stesso legislatore che, all'art. 3, comma 4-*bis*, individua l'AGCM quale autorità competente a verificare l'osservanza del divieto di *surcharge* e ad applicare le relative sanzioni, con la seguente formulazione: "L'Autorità garante della concorrenza e del mercato è designata quale autorità competente a verificare l'osservanza del divieto di cui al comma 4 e ad applicare le relative sanzioni, avvalendosi a tal fine degli strumenti, anche sanzionatori, previsti dal decreto legislativo 6 settembre 2005, n. 206". Dunque, per disposizione normativa, l'AGCM ha la competenza generale sul *credit surcharge*.

Sul piano delle conseguenze, si osserva, in primo luogo, che con ciò l'AGCM amplia la propria sfera di operatività al di là del rapporto professionista/consumatore, assumendo rilievo più l'attività e il servizio prestato che non la qualità soggettiva del contraente.

L'art. 3, comma 4-*ter*, dispone poi meccanismi di collaborazione tra AGCM e Banca d'Italia per agevolare l'esercizio delle rispettive funzioni. L'importanza della leale cooperazione tra *Authorities* è centrale per il buon funzionamento dell'attività di vigilanza; nel caso di specie, la Banca d'Italia e l'AGCM esercitano funzioni tra loro complementari, in ciò perseguendo interessi convergenti nello sviluppo e mantenimento di adeguati livelli di concorrenza nei mercati e tutela dei consumatori. Tale convergenza di interessi, pur nel rispetto dell'autonomia e dell'indipendenza delle rispettive funzioni, determina l'opportunità di instaurare rapporti di cooperazione per coordinare e rendere più efficace e incisiva l'esecuzione dei rispettivi mandati[17]. Sotto questo profilo, dunque, il decreto di attuazione della PSD2 traccia una strada importante per garantire l'*enforcement* della disciplina, che merita di essere apprezzata tanto più che, in generale, si registra una certa incoerenza tra la tendenza mostrata dalle Autorità europee e nazionali,

[17] In particolare, il principio di leale collaborazione rende necessario condividere informazioni e dati acquisiti nell'esercizio delle rispettive funzioni e competenze, in coerenza con il principio di buon andamento dell'azione amministrativa di cui all'art. 97 della Costituzione.

che cooperano fattivamente tra loro, e la resistenza opposta dalle autorità nazionali competenti per settori.

Il d.lgs. 15 dicembre 2017, n. 218, inserisce anche un nuovo art. 32-*quater* che, al comma 1, fatta salva l'applicazione dell'art. 62 del Codice del Consumo, prevede l'obbligo per le banche di informare gli utenti in merito ai costi dei prelievi di contante tramite sportelli automatici e, al successivo comma 2, demanda all'AGCM l'effettuazione dei controlli circa l'osservanza di tale obbligo da parte delle banche (cfr. art. 2, comma 38).

Viene data infine (art. 34-*quater*) all'AGCM la competenza ad inibire la continuazione e a rimuovere gli effetti delle pratiche commerciali scorrette e delle condotte in violazione della disciplina CRD (Direttiva 2011/83/UE) derivanti dall'inosservanza degli obblighi a carico dei beneficiari posti dal Regolamento (UE) n. 751/2015 - MIF (cfr. art. 3, comma 1), riconoscendole tutti i poteri che le sono attribuiti dall'art. 27 del Codice del Consumo. Si prevede, anche in questo caso, la collaborazione tra le due Autorità.

Da queste indicazioni normative viene fuori un sistema di vigilanza ben articolato in cui, in assenza di indicazioni in seno alla Direttiva, è il legislatore nazionale che ha provveduto a rimediare al silenzio del legislatore europeo. Si può affermare che la vigilanza sulla corretta applicazione delle disposizioni della PSD2 spetta alla Banca d'Italia con le eccezioni richiamate su cui è chiamata a intervenire l'AGCM.

Resta da stabilire se, escluso il contrasto tra norme e risolto il tema del *credit surcharge*, gli ambiti di sovrapposizione si esauriscano in quelli individuati dal legislatore oppure ne sussistano altri.

A ben vedere, la disciplina delle pratiche scorrette si può applicare ad ogni rapporto di consumo in cui il professionista abbia violato gli obblighi di diligenza professionale gravanti su di esso. In tali casi, il rispetto della disciplina settoriale diventa un parametro di riferimento ai fini della definizione del livello di diligenza che deve essere osservato dall'operatore in generale e dell'intermediario nella specie. In questa prospettiva, sembra potersi affermare che il ventaglio di possibili interventi dell'AGCM sia più ampio di quello individuato dal legislatore nel d.lgs. 218/2017, ma che, anche in tal caso, eventuali conflitti tra norme potrebbero essere risolti sulla base dei principi espressi dalla Corte di Giustizia, in una chiave di competenza concorrente funzionale.

In conclusione, con riguardo al rapporto tra Banca d'Italia e AGCM il d.lgs. 218/2017 attua un riparto di competenze tra decisori che mira a salvaguardare al meglio gli interessi dei clienti. Dove non arriva il legislatore,

è il quarto pilastro dell'Unione a soccorrere, cioè la Corte di Giustizia che interviene a supplenza del legislatore europeo, come ormai è consona fare, indicando la via da seguire[18].

4. *Un nuovo problema. Il rapporto tra PSD2 e GDPR*

Problema molto più grave, anche perché trascurato dal legislatore, è quello che investe il riparto di competenze tra Banca d'Italia e Garante Privacy.

A ben vedere, qui l'origine del problema è a monte: manca, infatti, un raccordo espresso tra la disciplina della PSD2 e quella del GDPR[19] e, almeno a prima lettura, vi è persino il rischio di ravvisare tra le due normative un'incompatibilità applicativa potenziale. Se, da un lato, il GDPR tutela il diritto alla protezione dei dati personali come un diritto fondamentale delle persone, ponendo come principio cardine l'autodeterminazione informativa, ossia il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano e tenta quindi di effettuare un bilanciamento tra circolazione e protezione del dato personale a garanzia della dignità delle persone, dall'altro lato, la PSD2 favorisce lo scambio e la condivisione di dati e informazioni tra diversi prestatori di servizi di pagamento rendendo facilmente accessibili dati personali dei clienti.

Uno dei più importanti cambiamenti attuati dalla PSD2 riguarda, infatti, come si è detto, il fatto che le banche devono consentire ai diversi *provider*s l'accesso ai dati dei clienti e ai conti, dando così luce al c.d. "*Open Banking*". La spinta tra innovazione e concorrenza in questa disciplina settoriale si traduce

[18] Si rinvia a quanto da me già rilevato in *La Corte di giustizia e il diritto dell'economia*, cit., p. 352 e cioè che: "Secondo l'insegnamento tradizionale, la Corte esercita il potere giurisdizionale svolgendo, al contempo, quando necessario: (i) un ruolo *normativo* (innova) quando interpreta il diritto applicando, ma anche *integrando*, gli atti legislativi ed esecutivi; (ii) un ruolo *evolutivo*, quando interpreta il diritto dell'UE lasciando, poi, ai giudici nazionali il compito di valutare la compatibilità del diritto interno con il diritto dell'UE; (iii) un ruolo di giudice di *appello* rispetto al tribunale di primo grado. Già da quanto si è fin qui detto, si evince che la Corte di Giustizia ha assunto un ruolo così forte da renderla alla stregua di un *legislatore aggiunto e forse davvero autonomo*. A queste funzioni se ne può aggiungere una ulteriore, che vede la Corte di Giustizia (iv) giudice dell'esecuzione, essendo l'unica che è in grado di dare effettivo contenuto alle disposizioni normative, nell'inerzia o inettitudine degli altri soggetti legittimati a farlo (legislatore, *Authorities)*".

[19] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

soprattutto nell'apertura del mercato dei servizi di pagamento alle c.d. *Third Party Providers* (cosiddette TPP, che si distinguono in "prestatori di servizi di disposizione di ordini di pagamento" e "prestatori di servizi di informazione sui conti") i quali, rispettivamente, possono avere accesso al conto del cliente che è radicato presso il prestatore di servizi (banca) per disporre pagamenti ai terzi beneficiari verificando l'esistenza dei fondi necessari; oppure, per aggregare le informazioni presenti su vari conti *online* e restituire al cliente la visione complessiva della propria situazione finanziaria, senza che il cliente debba contattare i vari prestatori di servizi di pagamento[20].

Con l'ingresso delle terze parti, cioè, il flusso dei dati derivanti da tutte le operazioni di pagamento si sposta dagli operatori bancari tradizionali ai TPP, che si frappongono tra cliente e operatore bancario e acquisiscono, al posto di quest'ultimo, tutte le informazioni relative alla transazione in atto[21]. La novità di PSD2 è di avere combinato il tema delle informazioni legate al conto di pagamento con quello della tecnologia che, attraverso il meccanismo delle APIs[22], consente l'interfaccia fra il mondo della banca e di altri operatori (PISP e AISP)[23].

Sul punto, la PSD2 (e il d.lgs. 218 che la attua) prevede una disciplina articolata e complessa relativa alle regole che devono essere osservate dai prestatori di servizi di pagamento per eseguire le prestazioni richieste quando sono coinvolte le cosiddette Terze parti.

Senza alcuna pretesa di esaustività si richiamano di seguito le principali regole.

L'art. 5 *bis* – concernente le condizioni necessarie per il soddisfacimento della richiesta di disponibilità dei fondi del cliente effettuata dalla Terza Parte al prestatore del servizio di radicamento del conto – prevede che

[20] Si deve trattare di soggetti autorizzati da Banca d'Italia che abbiano stipulato una assicurazione contro i danni (art. 144 *septies,* d.lgs. 19 settembre 1993, n. 385, Testo Unico delle leggi in materia bancaria e creditizia).

[21] Questo tema è di particolare rilevo in Italia dal momento che è l'unico Paese in cui la pratica del multi-affidamento è così diffusa e costituisce un problema serio.

[22] *Application Programming Interfaces* sono un insieme di protocolli che definiscono in che modo posso interagire le componenti dei *software*. A livello europeo, il Piano d'Azione della Commissione ha previsto, entro la metà del 2019, lo sviluppo, da parte di imprese e fornitori di nuove tecnologie, di interfacce di programmazione delle applicazioni (API) standardizzate e conformi a PSD2 e GDPR, alle quali gli altri operatori saranno tenuti ad adattarsi. L'obbiettivo è quello di giungere a una standardizzazione delle modalità di esecuzione dei pagamenti digitali e di rendere più sicure le transazioni ottenendo così una maggior tutela dei consumatori

[23] O. Borgogno – G. Colangelo, *Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy*, European Union Law Working Paper, Stanford – Vienna Transatlantic Technology Law Forum, 2018.

debba trattarsi di conto *online* e che il cliente debba avere prestato il suo consenso al titolare del servizio di radicamento del conto a dare conferma della disponibilità dei fondi al *provider* relativamente a una determinata operazione; mentre il prestatore di servizi di pagamento può chiedere la conferma – che non può consistere nell'estratto del saldo del conto – quando il pagatore ha prestato il consenso esplicito e ha disposto l'operazione di pagamento utilizzando uno strumento di pagamento basato su carta emesso dal prestatore di servizi di pagamento.

L'art. 5 *ter* disciplina, invece, il comportamento che deve essere adottato dal PISP in caso di servizi di disposizione di ordine di pagamento, regolando puntualmente anche l'uso che questi può fare dei dati di cui viene a conoscenza. Si prevede al riguardo che, se il conto di pagamento è accessibile *online*, il PISP non può detenere in alcun momento i fondi del pagatore e deve provvedere affinché le credenziali di sicurezza personalizzate del pagatore medesimo non siano accessibili ad altri fuorché al pagatore e affinché qualunque altra informazione sul pagatore ottenuta nella prestazione del servizio in discorso sia fornita esclusivamente al beneficiario e solo con il consenso esplicito del pagatore medesimo. Inoltre, il PISP, con riferimento specifico al trattamento dei dati di cui viene a conoscenza nel corso dell'operazione: (i) non chiede al pagatore dati diversi da quelli necessari per prestare il servizio di disposizione di ordine di pagamento; (ii) non usa e non conserva dati e non vi accede per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento; (iii) non conserva dati sensibili relativi ai pagamenti del pagatore. Ancora, per quanto riguarda gli obblighi in capo al prestatore di servizio di radicamento del conto in caso di disposizione di ordine di pagamento, la norma prevede che egli sia tenuto a comunicare con la terza parte in maniera sicura e a fornirle tutte le informazioni disponibili sull'ordine di pagamento.

All'art. 5 *quater* del d.lgs. 218/17 vengono introdotte, poi, alcune regole per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse nell'ipotesi di servizi di informazioni sui conti (AISP). In questo caso, l'AISP presta il proprio servizio unicamente sulla base del consenso esplicito dell'utente e provvede affinché le credenziali di sicurezza personalizzate dell'utente non siano accessibili ad altri fuorché all'utente stesso. Quanto al trattamento dei dati, l'AISP: (i) accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento effettuate a valere su tali conti, non richiedendo dati sensibili relativi ai pagamenti; (ii) non usa, non conserva dati, non vi accede per fini diversi dalla prestazione del servizio di informazione sui conti, conformemente alle norme sulla protezione dei dati.

L'art. 6 *bis* detta, infine, alcuni limiti all'accesso ai conti di pagamento da parte di PISP e AISP: in particolare, si prevede che il prestatore di radicamento del conto possa rifiutare l'accesso ai TPP solo per giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento da parte di tali soggetti. E, in questi casi, il medesimo è tenuto a informare l'utente del rifiuto e dei relativi motivi, nonché a darne immediata comunicazione a Banca d'Italia. Inoltre, il prestatore di radicamento del conto deve rifiutare senza indugio l'accesso se riceve dall'utente la revoca del consenso alla prestazione di tali servizi.

La presenza di tali norme impone all'interprete di svolgere alcune riflessioni di sistema sul rapporto tra PSD2, disciplina settoriale e verticale, e GDPR, disciplina generale e orizzontale. In mancanza di un raccordo espresso fra le due normative sussiste infatti, almeno a prima lettura, il rischio di ravvisare tra esse un'incompatibilità applicativa potenziale. In questa prospettiva, va innanzitutto rammentato che il GDPR tutela il diritto alla protezione dei dati personali come diritto fondamentale – il cui principio cardine è l'autodeterminazione informativa, ossia il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano – e ragiona nell'ottica del bilanciamento tra circolazione e protezione del dato personale a garanzia della dignità degli individui (basandosi sulla nota triade *consent/ownership/portability*)[24]. La PSD2 mira, invece, a favorire lo scambio e la condivisione di dati e informazioni tra diversi prestatori di servizi di pagamento rendendo facilmente accessibili dati personali dei clienti (e in questa prospettiva la parola chiave è *information* su cui si innestano i concetti di *collection/digitisation/repackaging/datafication*).

Una peculiarità non priva di conseguenze, sia teoriche sia pratiche, della disciplina introdotta dalla PSD2 è costituita, come si è detto, dal fatto che non è necessario che sussistano relazioni contrattuali tra i TPP e i prestatori di servizio di radicamento del conto. L'obiettivo di rafforzare la concorrenza nel settore dei servizi di pagamento si traduce cioè nell'imporre alle banche (e agli IP) una "collaborazione forzata" con i TPP, anche in assenza di precedenti relazioni contrattuali[25], obbligandole unicamente a

[24] È chiara in questo senso l'indicazione dell'art. 6, comma 1, lett. *f*), GDPR: il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione di dati personali. Il rispetto del limite posto da questa norma è dato dalla possibilità, in concreto, per l'interessato di essere sempre adeguatamente informato sul modo in cui i dati sono trattati, riconoscendo tra l'altro il diritto di controllare l'accesso ai propri dati.

[25] Se il conto è accessibile *online*, il pagatore ha sempre il diritto di avvalersi del servizio. I

predisporre un'infrastruttura tecnologica idonea a rendere possibile l'accesso alle informazioni e a gestire tutti i possibili rischi che ne conseguono.

La possibile mancanza di antecedenti relazioni contrattuali fra i soggetti coinvolti comporta conseguenze anche sotto il profilo del riparto interno della responsabilità in caso di operazioni di pagamento non autorizzate, ben potendo accadere che i rapporti tra i due prestatori siano regolati unicamente dalla legge.

Questa disciplina per i TPP si affianca all'unica regola che, nel d.lgs. 218/17, si occupa – peraltro con risultati piuttosto deludenti – di coordinare il trattamento dei dati personali da parte dei prestatori dei servizi di pagamento con la disciplina generale sulla *privacy*.

L'art. 29, comma 1, del d.lgs. 11/10 (così come modificato dall'art. 2, comma 34, del d.lgs. 218/17) prevede infatti che "i prestatori di servizi di pagamento" possano trattare dati personali ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti. La fornitura di informazioni a persone fisiche in merito al trattamento dei dati personali e ad altro trattamento avviene in conformità al decreto legislativo n. 196 (Codice privacy). In ogni caso, i prestatori di servizi di pagamento, in base a quanto dispone l'art. 29, comma 1 *bis*, "hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo previo consenso esplicito dell'utente". Si tratta, dunque, di una regola a più ampio spettro che vale per tutti i prestatori di servizi di pagamento e non limitatamente ai conti *online*. Il rapporto tra questa norma e quelle sopra richiamate sembra porsi cioè in una logica di genere a specie.

L'ultimo comma dell'art. 29, in particolare, contiene almeno due regole essenziali che valgono in tutti i casi: la prima è la necessità del consenso contrattuale che il prestatore di servizi di pagamento (sia esso prestatore di servizio di radicamento del conto oppure TPP) e il cliente devono avere manifestato reciprocamente; l'altra è il rispetto, anche a questo riguardo, del "principio di minimizzazione dei dati", in base al quale i prestatori di servizi di pagamento possono utilizzare, accedere, o conservare i dati acquisiti esclusivamente per la prestazione dei servizi tipici da essi offerti. Quest'ultimo principio, enunciato all'art. 5, lett. *c*), del GDPR, è peraltro uno di quelli maggiormente connotanti la disciplina generale del trattamento dei dati personali, tanto più che, come è stato rilevato in dottrina, non vi è dubbio che "meno dati si utilizzano meno rischi si fanno correre all'interessato"[26].

Se questo è, a grandi linee, il regime previsto a tutela del corretto

PISP hanno sempre l'obbligo di "identificarsi" presso gli ASPSP.

[26] F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale,* in *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino 2018, p. 62.

trattamento dei dati personali dalla PSD2, il confronto di tale normativa con il GDPR legittima alcuni interrogativi che hanno grande rilievo pratico. In particolare, occorre chiedersi: (i) quale sia, ai sensi del GDPR, la "base legittima" prevista per legge che consenta ai TPP il trattamento dei dati personali; (ii) quale sia la regola da adottare in presenza di dati "sensibili" cui possa accedere il TPP; (iii) come vadano ripartite le responsabilità tra prestatore di servizi di radicamento del conto e terze parti in caso di utilizzo illecito dei dati, dal momento che la PSD2, come si è detto, prevede che il servizio possa essere prestato all'utente indipendentemente dall'esistenza di un rapporto contrattuale con l'ASPS; (iv) quale criterio consenta di stabilire chi sia, tra prestatore del servizio di radicamento del conto e terze parti, il titolare del trattamento e chi il responsabile dello stesso[27]; (v) quale sia la regola da seguire e il meccanismo di protezione delle cosiddette parti silenti, ossia dei beneficiari dei pagamenti i cui dati "circolano" anch'essi nello svolgimento dell'attività; (vi) chi sia l'Autorità competente a vigilare sul rispetto delle regole imposte da PSD2 e GDPR, quando si effettua il servizio di pagamento in regime di *Open Banking*[28].

5. *Gli strumenti di tutela: il consenso*

Pur non potendosi in questa sede fornire una risposta esaustiva a tutte le questioni appena prospettate – con riguardo alle quali la soluzione non può che provenire dalla cooperazione fra le istituzioni europee maggiormente coinvolte –, si cercherà, nel prosieguo, di dare qualche indicazione utile a partire dalle prime indicazioni che provengono dall'Europa in proposito.

Con lettera del 5 luglio 2018 indirizzata al Parlamento Europeo, lo

[27] La figura del responsabile del trattamento è disciplinata compiutamente nell'art. 28 GDPR, che ne precisa i doveri chiarendo che è un soggetto terzo al quale il titolare ricorre per lo svolgimento di trattamenti che devono comunque essere fatti valere per suo conto e in suo nome. Il rapporto tra i due deve essere regolato da un contratto e il titolare è tenuto ad accertarsi che il responsabile offra garanzie adeguate ad assicurare che i trattamenti siano conformi al Regolamento.

[28] La questione non ha rilievo solo teorico: basti pensare che ai sensi dell'art. 83 GDPR, in caso di violazioni del Regolamento, il Garante per la protezione dei dati personali potrà irrogare una sanzione amministrativa pecuniaria fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore; tenendo in debito conto la natura, la gravità, la durata della violazione, il carattere doloso o colposo della stessa, le categorie di dati personali interessate dalla violazione, ecc.

European Data Protection Board (EPDB)[29] – che ha sostituito il WP29 – ha fornito alcune prime indicazioni volte al coordinamento delle due discipline. Si richiamano, perciò, qui di seguito le valutazioni dell'EDPB, nella consapevolezza che questa voce non basta a dare risposte se non è accompagnata dalla voce dell'EBA. In quest'ambito sembra, infatti, opportuno che la cooperazione tra le due *Authorities* trovi espressione in Standard tecnici o Linee Guida condivise.

Innanzitutto, nella lettera del 5 luglio 2018, l'EDPB chiarisce quale sia la corretta base legale per il trattamento dei dati personali effettuato da parte di un prestatore di servizi di disposizione di ordine di pagamento (PISP) che tratta i dati di un soggetto destinatario di un pagamento (la c.d. "parte silente") su ordine del cliente, posto che il consenso non lo ha ricevuto dalla "parte silente" (che non ha alcuna relazione contrattuale con lui), ma dal cliente. Ad avviso dell'EDPB, l'interesse legittimo del titolare e responsabile del trattamento è sufficiente base legale per il trattamento, purché vengano rispettati i principi di minimizzazione, limitazione e trasparenza e quei dati vengano usati solo per tale finalità di trattamento, in linea con quanto previsto dall'art. 6, paragrafo 1, lett. *f*), del GDPR. Il limite è, dunque, dato dalla violazione degli interessi e dei diritti fondamentali dell'interessato.

Un secondo profilo su cui si esprime l'EDPB è quello del significato da attribuire nelle due discipline alla formula "consenso esplicito": si intende, cioè, stabilire se il consenso richiesto dal GDPR possa essere il medesimo imposto dalla PSD2 per l'operatività dei TPP. Si è rilevato che: "natura, funzione e finalità di tali due manifestazioni di «adesione» non sono del tutto omogenei e sovrapponibili nella dinamica dei rispettivi plessi disciplinari, ciò considerato ad esempio anche che, come noto, mentre il GDPR reca un corpus di norme relativo alla protezione delle «persone fisiche» (identificate o identificabili – cosiddetti «interessati») con riguardo al trattamento dei loro «dati personali», nonché alla libera circolazione dei dati stessi, in quest'ambito il focus della PSD 2 è piuttosto sulla protezione dei dati degli «utenti» in genere di servizi di pagamento"[30].

Sostiene l'EDPB che, mentre il consenso indicato dal suddetto art. 94, paragrafo 2, della PSD2 (recepito in Italia all'art. 29 del d.lgs. 218/17) è un consenso di natura contrattuale che lega il prestatore di servizi di pagamento

[29] Lo *European Data Protection Board* è il coordinamento tra i garanti nazionali dell'Unione, cui partecipa anche il Garante europeo per la protezione dei dati e una rappresentanza della Commissione. Il Gruppo formula raccomandazioni, stabilisce *standard* comuni, emette pareri su questioni tecniche per gli Stati membri e per la Commissione europea.

[30] A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services*, in *Quaderni, Consob*, Marzo, 2019, p. 33.

e il cliente ed è un consenso limitato al tipo di servizio di pagamento da svolgersi, il consenso richiesto dal GDPR è più generale. Ciò induce a ritenere che il consenso GDPR riguardi il trattamento di qualsiasi altro dato, anche non strettamente necessario per l'esecuzione del contratto, purché si rientri nell'ipotesi dell'art. 6, paragrafo 1, lett. *a*) del GDPR e siano rispettate le condizioni richieste per il consenso dell'interessato dall'art. 7 dello stesso Regolamento.

Il consenso della PSD2 è, pertanto, funzionale alla sola prestazione del servizio di pagamento e ad essa limitato; solo in questo stretto perimetro sostituisce, perciò, il consenso GDPR che rimane, invece, necessario per tutte le ulteriori finalità che il titolare del trattamento è autorizzato a perseguire, purché si rispettino i limiti imposti dal GDPR e le modalità con cui esso deve essere raccolto[31].

Questo aspetto consente anche di dare conto di quale comportamento i TPP debbano adottare quando vengono a conoscenza di "dati sensibili". Al riguardo si rileva che nella PSD2 manca una nozione di "dati sensibili" che, con formulazione lata, sono identificati in quelli "relativi ai pagamenti che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate". Si prevede, però, come si è detto, che il PISP non possa trattare né conservare dati sensibili del cliente e l'AISP neppure possa richiederli.

Le norme pongono un divieto e, per l'effetto, stabiliscono un limite alla disponibilità negoziale delle parti, non superabile attraverso il consenso. L'obiettivo è la tutela dell'interesse della clientela a non essere vittima di frodi.

[31] In questa prospettiva sembra corretta la lettura offerta da A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *op. cit.,* p. 35, secondo cui verrebbe così a "delinearsi una disciplina differenziata, segnatamente nel senso della previsione di una *protezione extra* o *rafforzata*, per il *trattamento* di "dati personali" nell'ambito della prestazione dei servizi di "*informazione sui conti*", in quanto, ai sensi dell'art. 94, par. 2, della PSD 2, un "*consenso esplicito*" e specifico dei relativi "*utenti*" sembra invece essere sempre necessario, sicché è lasciato all'interprete (e alle Autorità) il compito di stabilire se anche in tale contesto casi trovi applicazione oppure no, e in che misura, l'autonoma e generale condizione di liceità del *trattamento* dei *dati personali* di cui all'art. 6, par. 1, lett. b), del *GDPR*. Partendo dall'assunto che in generale le norme della PSD 2 in materia di protezione dei *dati personali* e quelle del *GDPR* sono da interpretare e applicare in modo il quanto più possibile coordinato e coerente, una possibile lettura del risultante "combinato disposto" potrebbe essere pertanto quella secondo cui la necessità del «*consenso esplicito*» di cui all'art. 94, par. 2, della PSD2 sarebbe invero da intendere nel senso che, da un lato, gli AISPs hanno l'obbligo di mantenere informato l'*utente* dei servizi di "informazione sui conti" circa le *finalità* della raccolta e successivo specifico *trattamento* dei suoi dati personali «*necessari alla prestazione dei rispettivi servizi*», dall'altro, che l'*utente* stesso debba acconsentire esplicitamente a tali *finalità* e *trattamento* e ciò soprattutto ai sensi e per gli specifici effetti delle norme speciali di settore di cui alla PSD 2".

È evidente qui l'assenza di raccordo con il GDPR, in cui la nozione di dato sensibile è centrale, ma assume un significato completamente diverso, facendosi riferimento ai dati relativi a origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; dati genetici o biomedici; dati relativi alla salute o all'orientamento sessuale della persona.

Un'ulteriore questione trattata dall'EDPB concerne, poi, le API, con riguardo alle quali ci si interroga sul fatto che le medesime siano sufficientemente sicure e idonee a soddisfare il livello di protezione richiesto dal GDPR. Sotto questo profilo, l'EDPB valorizza il ruolo delle Autorità nazionali di vigilanza sulla protezione dei dati personali attribuendo a loro la vigilanza sul fatto che: "il titolare del trattamento e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio" (art. 32 GDPR).

Muovendo da queste indicazioni, si possono svolgere un paio di considerazioni ulteriori sotto due profili: (i) il ruolo che assumono AISP e PISP come titolari e/o responsabili del trattamento ai sensi del GDPR[32]; (ii) quali siano le misure che devono essere adottate per prevenire *data breach* e utilizzo illecito dei dati.

La diversa rilevanza del consenso ai fini PSD2 e GDPR porta a ritenere che qualora il TPP chieda l'accesso ai dati possono delinearsi due diversi scenari. Nel caso in cui, non solo intercorra una relazione contrattuale (regolata con consenso espresso, secondo le regole settoriali della PSD2) tra l'interessato e il TPP avente ad oggetto un servizio di disposizione di ordine di pagamento o di informazione sui conti, ma sussista anche un rapporto contrattuale pregresso tra prestatore del servizio di radicamento del conto e TPP, il consenso all'interessato va richiesto da chi effettua il trattamento[33]. Ciò a meno che l'accordo sussistente tra prestatore del servizio di radicamento del conto e TPP stabilisca in via negoziale chi fra i soggetti coinvolti sia il titolare e chi il responsabile del trattamento e preveda un criterio di riparto della responsabilità in caso di frode, utilizzo illecito dei dati e *data breach*, in generale. Nell'accordo potrebbe essere anche stabilito chi è tenuto a comunicare l'incidente all'Autorità competente.

Nel caso invece, verosimilmente più frequente, in cui non preesista

[32] Come ha affermato F. Pizzetti, *op. cit.*, p. 46, il titolare del trattamento è "la pietra angolare e il perno di tutto il sistema di protezione dei dati personali": egli risponde del modo in cui tratta i dati dell'interessato, ha il dovere di informare l'interessato dei trattamenti in corso e di applicare a questi il principio di trasparenza, deve assicurare la tutela dei dati e la protezione dei diritti e delle libertà fondamentali delle persone fisiche.

[33] Purché sia assicurato il rispetto della regola sul consenso GDPR, come configurata dagli artt. 6 e 7 del Regolamento.

alcuna relazione contrattuale tra ASPSP e TPP, la questione è più complessa ed entrambi i soggetti potrebbero essere considerati titolari del trattamento. Certamente, ai fini del GDPR, è titolare dei dati chi effettua l'uso secondario degli stessi: quindi, in questa prospettiva, titolare risulta il TPP, mentre utilizza i dati ai fini degli adempimenti degli obblighi contrattuali.

6. *(*Segue*). L'accountability*

Ma se il consenso è essenziale ai fini del legittimo trattamento dei dati per gli obiettivi della PSD2 e del GDPR esso, tuttavia, non è sufficiente a evitare che possa aversi un uso illecito dei dati o che possa verificarsi un incidente relativo ad essi, eventi rispetto ai quali occorre individuare ulteriori strumenti di tutela a carattere preventivo.

Il passaggio da un adempimento "formale" (quale la raccolta e prova del consenso del cliente) a una "sostanziale" strategia di azione da parte sia degli ASPSP sia dei TPP è, quindi, fondamentale e consiste nell'adozione di presidi organizzativi e procedure adeguate a prevenire i rischi connessi all'attività di prestazione di servizi di pagamento *online* e al trattamento dei dati personali dei clienti.

In questa prospettiva, non va dimenticato che, nel contesto del GDPR, il principio dell'*accountability* riveste un ruolo determinante: ai titolari del trattamento è demandato, infatti, il compito di decidere in autonomia modalità e limiti del trattamento dei dati e a loro viene imposto di organizzarsi con procedure e protocolli idonei all'obiettivo di prevenzione dei rischi che possono derivare dal trattamento dei dati e che vanno sempre commisurati ai diritti e alle libertà personali[34]. Più in dettaglio, l'art. 24

[34] Al tema della protezione e quindi della sicurezza dei dati appartiene il complesso di disposizioni che pongono a carico del titolare l'obbligo di dare avviso prontamente delle violazioni dei dati (artt. 33 e 34); l'obbligo di compiere una preventiva valutazione dei possibili rischi, anche consultando preventivamente l'autorità di controllo (artt. 35 e 36); l'obbligo di designare, in relazione a trattamenti effettuati da soggetti pubblici ovvero aventi ad oggetto particolari categorie di dati, un responsabile della protezione dei dati (art. 37), del quale il Regolamento individua (art. 39) i compiti in maniera dettagliata. A questo novero di obblighi si aggiunge, poi, un ulteriore complesso di regole che, sul piano volontario, prevedono l'adesione a codici di condotta elaborati autonomamente dalle associazioni di categoria (art. 40) ed ancora l'eventuale sottoposizione ad un organismo di vigilanza indipendente, con procedure di certificazione delle misure adottate per la protezione dei dati, affidate ad autonomi organismi di certificazione (artt. 42 e 43) accreditati, al pari

GDPR definisce la responsabilità del titolare del trattamento, chiarendo che questi deve sempre – sia prima di iniziare un trattamento, sia durante il suo svolgimento – "mettere in atto misure tecniche e organizzative adeguate a garantire, e essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento"[35]. Di conseguenza, anche alla luce dell'art. 82 GDPR, il titolare coinvolto nel trattamento risponde in solido per il danno cagionato in violazione del GDPR a meno che non dimostri che l'evento dannoso non gli è imputabile. Particolare rilievo assume, a tal fine, la "Valutazione d'impatto sulla protezione dei dati" (DPIA) disciplinata dall'art. 35, necessaria qualora un certo trattamento necessiti di un'ulteriore valutazione in considerazione di un rischio specifico (specie in caso di uso di nuove tecnologie) e renda opportuna l'adozione di altre puntuali misure di sicurezza e prevenzione dei rischi[36]. Nel caso dell'*Open Banking* con accesso e gestione dei dati da parte dei TPP, questa ulteriore valutazione di rischio può risultare opportuna.

Si valorizza così la discrezionalità dell'intermediario e delle terze parti nel predisporre procedure e cautele specifiche idonee a contrastare il verificarsi del rischio dell'uso illecito dei dati. Spetta, quindi, al titolare del trattamento l'onere di dimostrare la bontà delle proprie scelte organizzative cui si lega un regime di responsabilità rafforzata se le misure adottate non dovessero rivelarsi adeguate sotto il profilo della tutela dei dati imposta dal GDPR.

L'*accountability* è, peraltro, espressione del principio più generale dell'adeguatezza degli assetti organizzativi d'impresa, criterio cardine intorno a cui ruota la regola di responsabilità della gestione dell'impresa sia nella legislazione settoriale bancaria e finanziaria, sia nel Codice civile agli art. 2380 ss.

Allargando lo sguardo in questa direzione, ragionare in termini generali

degli organismi di vigilanza, presso l'Autorità garante. Sul valore dell'*accountability*, v. L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in *Innovazione tecnologica e valore della persona*, a cura di L. Califano e C. Colapietro, Napoli 2018, p. 14 ss.

[35] V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa Eur.*, 2018, p. 1115, secondo cui: "la prescrizione di obblighi specifici, e specificamente sanzionabili ai sensi dell'art. 83 del Regolamento, viene a spostare il baricentro della disciplina mettendo l'accento sulla necessità di limitare preventivamente il rischio insito nel trattamento dei dati personali. La necessaria adozione di misure preventive, dirette a realizzare il rispetto delle regole di trattamento ed insieme a ridurre il rischio di pregiudizi, determina così una sorta di positivizzazione degli obblighi di protezione".

[36] Il WP29 nelle *Guidelines on data protection impact assessment* afferma che la DPIA è necessariamente successiva ed eventuale rispetto alla valutazione del rischio dell'art. 24 che costituisce secondo F. Pizzetti, *cit.*, p. 63 "l'architrave" di tutto il Regolamento GDPR.

di prevenzione e gestione integrata dei rischi di impresa sembra utile anche per tutelare gli ulteriori interessi riconducibili agli obiettivi propri della PSD2 (favorire la circolazione dei dati e lo *sharing* degli stessi tra i diversi operatori). La gestione integrata dei rischi di impresa[37] è un'esperienza che dimostra, infatti, come ogni nuovo rischio specifico debba essere considerato dal complessivo sistema dei controlli interni e debbano, con riguardo ad esso, essere predisposte procedure atte a prevenire il suo concretizzarsi.

In questa prospettiva, il più efficace strumento per realizzare il coordinamento fra PSD2 e GDPR e per contrastare il rischio di utilizzo illecito dei dati senza tuttavia mortificare la spinta all'apertura e alla concorrenza nel settore dei servizi di pagamento potrebbe rinvenirsi proprio nell'*accountability*, regola trasversale di responsabilizzazione del prestatore di servizi di pagamento, sia esso ASPSP o TPP. In altri termini, lo strumento per tenere insieme le diverse finalità dei due provvedimenti normativi potrebbe essere quello dell'efficiente organizzazione d'impresa in chiave di prevenzione dei rischi; spetta all'impresa, cioè, dimostrare di avere adottato presidi, protocolli e misure organizzative idonee a soddisfare i requisiti richiesti dal Regolamento GDPR senza ostacolare lo sviluppo dell'*Open Banking*.

7. *Conclusioni: verso una competenza concorrente tra* Authorities

L'analisi sin qui condotta induce peraltro a concludere che, per quanto le difficoltà di coordinamento tra le due discipline siano numerose e significative e impongano indirizzi interpretativi unitari e soluzioni tecniche condivise a livello europeo, non si registrano davvero "contrasti tra disposizioni" tali da incidere sulla questione del riparto di competenze tra *Authorities* di vigilanza. E ciò quantomeno se si accoglie l'accezione di "contrasto" come effettiva antinomia fatta propria dalla Corte di Giustizia con la decisione del 13 settembre 2018 che, pur riferendosi a una diversa fattispecie, può rivelarsi un'utile guida alla soluzione del problema. La Corte di Giustizia ha chiarito, infatti, che un problema di riparto di competenze tra *Authorities* può porsi solo laddove sussista un "contrasto" tra le disposizioni

[37] Il concetto di Gestione integrata del rischio di impresa ha l'obiettivo di massimizzare l'efficienza del sistema di controllo interno e ridurre le duplicazioni di attività e il controllo strategico dei rischi. Le componenti del controllo devono essere coordinate e interdipendenti e il sistema nel complesso deve essere integrato nell'assetto organizzativo, amministrativo e contabile della società.

applicabili, da ravvisarsi quando "il rapporto tra due disposizioni va oltre la mera difformità o la semplice differenza, mostrando una divergenza che non può essere superata mediante una formula inclusiva che permetta la coesistenza di entrambe le realtà, senza che sia necessario snaturarle".

Quanto detto, seppure in modo sintetico, è utile per stabilire come operare, in questa materia, il riparto di competenze tra Banca d'Italia e Garante Privacy. In linea con l'indicazione della Corte di Giustizia si può ritenere che vi sia una competenza concorrente tra le due Autorità preposte, in chiave funzionale alla tutela degli interessi protetti[38]. Se l'interesse leso è la riservatezza del dato, interviene il Garante Privacy; se invece è violata la disciplina di PSD2 (violazione della regola del consenso contrattuale; mancanza dei presidi necessari per assicurare la *strong authentication*, ecc.) interviene Banca d'Italia.

L'avere rafforzato con PSD2 i poteri ispettivi del Garante Privacy[39] rende, peraltro, il ragionamento sin qui svolto rilevante anche sotto il profilo dell'*enforcement*, dal momento che le ispezioni possono diventare il "braccio armato" del Garante, come da sempre lo sono per Banca d'Italia.

Ma perché tutto ciò possa in concreto funzionare occorre che le autorità si attengano al principio di leale cooperazione tra loro, in modo da assicurare efficacia ed effettività all'azione coordinata e, per l'effetto, bilanciare al meglio gli interessi diversi ma comunque meritevoli di protezione.

Ove, invece, si ravvisasse per qualche verso un "contrasto reale" tra le due normative, un tale contrasto non potrebbe che essere risolto a livello

[38] Nel senso di ammettere anche un doppio procedimento e un doppio binario sanzionatorio ormai si orienta peraltro tutta la giurisprudenza di legittimità che si è pronunciata più volte di recente sul diverso tema del *cumulo dei procedimenti e ne bis in idem*, in caso di procedimento di opposizioni a sanzioni irrogate da Banca d'Italia e Consob. La scelta della giurisprudenza è stata nel senso di non escludere, in linea di principio, la possibilità di sanzionare diversamente illeciti per loro natura capaci di ledere contemporaneamente interessi diversi a cui garanzia sono preposte autorità diverse, purché sia rispettato il principio di *proporzionalità* delle sanzioni secondo il quale esse devono essere parametrate alla gravità del comportamento, ma non devono eccedere quanto necessario al fine di garantire la finalità della norma. Questo principio, che richiede la necessità, adeguatezza e proporzionalità della sanzione rispetto al fine, assume dunque assoluta centralità, divenendo il parametro per valutare il limite oltre il quale una qualsiasi disposizione non persegue più il proprio obiettivo.

[39] La centralità della figura del Garante quale perno intorno al quale ruota la disciplina della circolazione dei dati personali è ribadita nel Regolamento nell'art. 58, in cui sono riepilogate le funzioni delle quali è titolare il Garante, con riferimento a poteri di indagine, correttivi, autorizzativi e consultivi accompagnate dal significativo riconoscimento della legittimazione ad "intentare un'azione o agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso". Per un approfondimento, v. V. Cuffaro, *cit.*, p. 1118.

europeo, mediante Standard tecnici condivisi o Linee Guida congiunte emanate da EBA ed EDPB.

Abstact
La Direttiva sui servizi di pagamento (PSD2) innova profondamente la disciplina bancaria per garantire maggiore efficienza, concorrenza e trasparenza nell'offerta di servizi di pagamento. La principale innovazione è rappresentanta dall'open banking, che apre il mercato dei servizi di pagamento ai nuovi operatori. Altra innovazione significativa è il divieto di surcharge, che si estende al di là del settore in cui era già regolato nel Codice dei consumatori. Queste nuove regole pongono un problema di sovrapposizione tra diversi silos verticali e orizzontali. Il presente documento affronta la questione della ripartizione delle competenze tra le Autorità. In particolare, si concentra sul rapporto tra BANKIT, AGCM, Privacy.

Parole Chiave: Riparto; competenze; intersezioni; sovrapposizioni; silos.

Abstact
The Directive on payment services (PSD2) deeply innovates banking rules to guarantee greater efficiency, competition and transparency in the offer of payment services. The main innovation consists of open banking which opens the market for payment services to new operators. Another relevant reform is the prohibition of a credit surcharge which extends beyond the sphere in which it was already regulated in the Consumer Code. These new rules pose an overlapping problem between different vertical and horizontal silos. This paper deals with the issue of the division of competences between the Autorithies. In particular, it focuses on the relationship between BANKIT, AGCM, Privacy.

Keywords: Overlapping; surcharge; competence; Authorities; privacy.