Salvatore Sica e Benedetta Maria Sabatino **

Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore *

SOMMARIO: 1. I servizi di pagamento nel sistema comunitario. – 2. Ambito di applicazione della PSD2. – 3. La tutela dell'utente nell'ordinamento italiano: profili applicativi nella giurisprudenza dell'Arbitro Bancario Finanziario. – 4. Riflessioni di sintesi.

1. I servizi di pagamento nel sistema comunitario

Negli ultimi anni, il settore dei servizi di pagamento è stato oggetto di regolamentazione da parte del legislatore comunitario che, come è noto, è intervenuto, dapprima, con la direttiva 2007/64/CE – comunemente nota con l'acronimo PSD (*Payment Service Directive*) – e, più di recente, con la direttiva 2015/2366/UE – c.d. PSD2 (*Payment Service Directive 2*) [1].

---

* Il presente contributo riproduce, con alcune integrazioni, l'intervento svolto in occasione del seminario "*Financial Innovation tra Disintermediazione e mercato*" tenutosi a Roma in data 3 dicembre 2019.

** Lo scritto, pur se unitariamente concepito, è tuttavia da attribuire a Salvatore Sica per i paragrafi 1 e 4 a Benedetta Maria Sabatino per i paragrafi 2 e 3.

[1] In riferimento alla PSD v. O. TROIANO, *Contratto di pagamento*, in *Enc. dir.*, *Annali*, V, 2012, p. 392 ss.; M. MANCINI, M. RISPOLI FARINA, V. SANTORO, A. SCIARRONE ALIBRANDI, O. TROIANO (a cura di), *La nuova disciplina dei servizi di pagamento*, Giappichelli, Torino, 2011; M. RISPOLI FARINA, V. SANTORO, A. SCIARRONE ALIBRANDI, O. TROIANO (a cura di), *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, Giuffrè, Milano, 2009; M. MANCINI, M. PERASSI (a cura di), *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, in Banca d'Italia, Quaderni di Ricerca Giuridica della Consulenza Legale, n. 63, dicembre 2008. In relazione alla PSD2, si rinvia a: M.C. PAGLIETTI, M.I. VANGELISTI (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, Roma Tre-Press, 2020; G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Zanichelli, Bologna, 2019; F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, in

La nuova disciplina, a ben vedere, non stravolge il quadro normativo precedente, piuttosto lo integra e, dunque, va intesa come espressione della necessità di adeguare il quadro normativo europeo al fenomeno della *digital revolution* che ha determinato la nascita e lo sviluppo della c.d. *Fintech*[2].

Il primo provvedimento menzionato – recepito nel nostro ordinamento mediante il d.lgs. n. 11/2010 e con talune modifiche apportate al d.lgs. n. 385/1993 – va letto come il segno della volontà delle istituzioni europee (in particolare del Consiglio europeo per i pagamenti) di dare vita ad un mercato unico europeo dei pagamenti al dettaglio (c.d. SEPA – *Single Euro Payments Area*)[3].

Alla base della PSD, infatti, v'era proprio l'intenzione di predisporre regole uniformi in ordine ai pagamenti elettronici in tutta l'Eurozona. Il ruolo sempre più preminente assunto dai pagamenti elettronici – accanto quelli in denaro contante e tramite assegni – ha indotto il legislatore europeo a dettare regole omogenee improntate alla trasparenza ed alla sicurezza e volte a promuovere la fiducia nell'utilizzo degli strumenti di pagamento elettronici[4]. A tal uopo, l'ambito soggettivo di applicazione ha ricompreso, oltre agli enti creditizi tradizionali, anche gli istituti di pagamento e gli istituti di moneta elettronica.

Banca d'Italia, Quaderni di Ricerca Giuridica della Consulenza Legale, n. 87, settembre 2019. Sul rapporto tra PSD e PSD2, v. D. GAMMALDI, *La sicurezza degli strumenti e del mercato dei pagamenti*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, cit., p. 153 ss., spec. p. 156. L'A. ritiene che «il *fil rouge* che sottende le scelte regolamentari operate dalla Direttiva è favorire lo sviluppo tecnologico in un contesto di certezza, fiducia e sicurezza in cui la definizione dei servizi di pagamento è neutra sotto il profilo tecnologico per 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"».

[2] V.M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, Cedam, Milano, 2020. G. ALPA, *Fintech: un laboratorio per i giuristi*, in *Contr. imp.*, 2, 2019, p. 377 ss.; G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, cit., *passim*.

[3] O. TROIANO, *La nuova disciplina privatistica comunitaria dei servizi di pagamento: realizzazioni e problemi della* Single Euro Payments Area *(*SEPA*)*, in *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, cit., p. 41 ss.; F. MAIMERI, *I Rulebook della SEPA: natura e funzioni*, *ivi*, p. 123 ss.; M. MANCINI, *I sistemi di pagamento* retail *verso la* Single Euro Payments Area (SEPA), *ivi*, p. 243 ss.

[4] Considerando 4, direttiva 2007/64/CE: «È pertanto essenziale istituire un quadro giuridico comunitario moderno e coerente per i servizi di pagamento, siano essi compatibili o meno con il sistema derivante dall'iniziativa del settore finanziario a favore della creazione di un'area di pagamento unica in euro, che risulti neutrale in modo da garantire parità di condizioni per tutti i sistemi di pagamento, mantenendo così la libertà di scelta dei consumatori, e che rappresenti un chiaro progresso in termini di costi per i consumatori, nonché di sicurezza e di efficacia rispetto ai sistemi attualmente esistenti a livello nazionale».

Ciò, peraltro, ha consentito di interpretare la direttiva non soltanto dalla prospettiva concorrenziale, ma anche da quella inerente alla tutela del consumatore nel sistema comunitario [5].

Tuttavia, atteso che anche il settore dei pagamenti è stato interessato dall'evoluzione tecnologica, in poco meno di un decennio, la direttiva ha mostrato di essere poco attuale e, in parte, inadeguata rispetto al fenomeno dell'*open banking* e all'ingresso in tale ambito di altri *players* che prima ne erano esclusi (nonostante l'ampliamento dell'ambito soggettivo di applicazione dalla stessa già operato).

Va sottolineato che il proliferare di nuove modalità di pagamento e dei relativi prestatori di servizi – ormai operanti al di fuori dell'ambito strettamente bancario – ha richiesto un ulteriore intervento legislativo volto a distinguere i diversi servizi messi a disposizione dell'utenza e, di conseguenza, a prevedere dei livelli di sicurezza idonei a garantire alla clientela *standard* più elevati, diretti prevenire l'utilizzo fraudolento dei sistemi di pagamento.

Tali obiettivi sono posti al centro della direttiva 2015/2366/UE (integrata dal regolamento delegato 2018/389/UE), che, come noto, a livello nazionale, è stata recepita con d.lgs. n. 218/2017 ed ha modificato alcune disposizioni del Testo Unico Bancario e del citato d.lgs. n. 11/2010 [6].

La rivoluzione digitale nel settore dei pagamenti ha dunque richiesto

---

[5] V.O. TROIANO, *La nuova disciplina privatistica comunitaria dei servizi di pagamento: realizzazioni e problemi della* Single Euro Payments Area *(*SEPA*)*, cit., p. 40 ss., e M. GRANIERI, *Le liberalizzazioni nel sistema dei servizi di pagamento e l'impatto della direttiva comunitaria sull'industria delle carte di credito. Alcune riflessioni preliminari*, *ivi*, p. 96 ss.

[6] Il menzionato d.lgs. di recepimento è stato recentemente corretto ed integrato da un ulteriore d.lgs., come annunciato nel Comunicato stampa del Consiglio dei Ministri n. 39 del 6 aprile 2020. Nel comunicato si legge che «il decreto realizza un più chiaro e stretto allineamento tra le disposizioni della direttiva PSD2 e le norme nazionali e prevede, tra l'altro:

– il diritto di regresso nell'ipotesi in cui la responsabilità di un prestatore di servizi di pagamento sia attribuibile ad un altro prestatore di servizi di pagamento coinvolto o ad un qualsiasi altro soggetto interposto nell'esecuzione dell'operazione. In base alle nuove norme, il secondo prestatore di pagamento (coinvolto o interposto) dovrà risarcire il primo in caso di perdite o di importi versati con riferimento ad operazioni di pagamento non autorizzate e con riferimento alla mancata, inesatta o tardiva esecuzione delle operazioni di pagamento;

– l'iscrizione, ad opera della Banca d'Italia, in appositi albi, degli istituti autorizzati nonché delle succursali stabilite in uno Stato membro diverso dall'Italia;

– l'esclusione, per chi fornisce esclusivamente servizi di informazione sui conti, dell'obbligo di adozione di sistemi di risoluzioni alternative delle controversie;

– l'inclusione nell'elenco delle fattispecie sanzionabili dei casi di inosservanza, da parte degli agenti in attività finanziarie, degli obblighi in materia di credito immobiliare ai consumatori;

– l'ampliamento dell'ambito di applicazione delle sanzioni previste per la violazione delle norme sulla trasparenza bancaria anche a quelle relative all'inosservanza del regolamento sui costi dei servizi interbancari».

l'introduzione di regole altrettanto innovative [7] «al fine di colmare le lacune regolamentari, garantendo al contempo maggiore chiarezza giuridica e un'applicazione uniforme del quadro legislativo in tutta l'Unione [8]».

In particolare, la PSD2, ponendo in evidenza la crescita dei pagamenti elettronici e delle differenti modalità mediante le quali essi si effettuano, ha inteso ampliare il novero dei "prestatori di servizi di pagamento" e, di conseguenza, ha predisposto misure di sicurezza più rigide rispetto a quelle indicate nella precedente direttiva [9].

2. Ambito di applicazione della PSD2

Per quanto attiene al primo profilo, l'ambito soggettivo di applicazione ricomprende Banche, Istituti di Moneta Elettronica (IMEL), Istituti di Pagamento (IP), nonché le imprese, diverse dalle banche e dagli istituti di moneta elettronica, autorizzati a prestare i servizi di pagamento dall'Autorità di Vigilanza [10].

Pertanto, la disciplina non si riferisce più soltanto ai tradizionali enti creditizi e IP, ma si estende ad una serie di soggetti ulteriori che, proprio sfruttando le potenzialità delle nuove tecnologie (quali *smartphone*, altri *devices* e relative *app*), consentono, tra le altre cose, di superare i pagamenti mediante denaro contante o con carta e di ampliare il settore dei pagamenti elettronici [11].

---

[7] Considerando 3, direttiva 2015/2366/UE: «La direttiva 2007/64/CE è stata adottata nel dicembre 2007, sulla base di una proposta della Commissione del dicembre 2005. Da allora, con la rapida crescita del numero di 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».

[8] Considerando 6, direttiva 2015/2366/UE.

[9] In argomento, A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, cit., p. 13 ss.

[10] In relazione all'estensione dell'ambito di applicazione soggettivo della direttiva in esame, v. A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2*, cit., p. 15 ss.; S. BALSAMO TAGNANI, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2*, in *Contr. imp. eur.*, 1, 2018, spec. p. 610 ss.; V. PROFETA, *I Third Party Provider: profili soggettivi ed oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit., p. 49 ss.

[11] In proposito, si rinvia alle considerazioni di V. ZENO-ZENCOVICH, *Prefazione*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, cit., p. 9, che, nell'analizzare gli "effetti sistemici" della PSD2, individua, in primo luogo, «la presa d'atto della ormai irreversibile avanzata di sistemi interamente digitali, con la completa dematerializzazione della moneta. Un pro-

La direttiva – dopo avere indicato le tipologie di pagamenti escluse dal suo ambito applicativo [12] – muovendo dalla tipologia del servizio messo a disposizione dell'utenza da parte dei soggetti non finanziari (cc.dd. TTP – *Third Party Providers*), fornisce la definizione di "servizio di disposizione di ordine di pagamento" (PIS – *Payment Initiation Service*), inteso come quello con cui si «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» [13] (art. 4, comma 1, n. 15). Al contempo, il legislatore si è preoccupato di fornire una definizione di "servizio di informazione sui conti" (AIS – *Account Information Service*) consistente in un servizio *online* che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento [14].

Tra l'altro, nell'ambito servizi forniti dai TTP va annoverato anche quello di conferma della disponibilità dei fondi (*ex* art. 65). Trattasi di un servizio

---

cesso che è iniziato molti anni orsono – circa un trentennio – e che è facile prevedere avrà ulteriori sviluppi tecnologici e dunque regolamentari. Beninteso si tratta solo di una tappa nella millenaria storia della moneta, e che dunque va vista senza indulgere nella neolatria. Dal metallo alla carta ai bit la strada è lunga, ed ogni passaggio implica oltre a opportunità anche rischi che non possono e non devono essere sottovalutati, ed in effetti non lo sono nella Direttiva».

[12] Cfr. i considerando 11 e 16 ss., nonché l'art. 3, direttiva 2015/2366/UE.

[13] Cfr. considerando 29, direttiva 2015/2366/UE: «I servizi di disposizione di ordine di pagamento consentono al prestatore di servizi di disposizione di ordine di pagamento di assicurare al beneficiario che il pagamento è stato disposto così da incentivare il beneficiario a consegnare i beni o a prestare il servizio senza indebiti ritardi. Tali servizi offrono una soluzione a basso costo per i commercianti e i consumatori e consentono a questi ultimi di fare acquisti online anche senza carte di pagamento. Poiché non sono attualmente soggetti alla direttiva 2007/64/CE, i servizi di disposizione di ordine di pagamento non sono necessariamente soggetti alla vigilanza di un'autorità competente e non devono rispettare i requisiti di cui alla direttiva 2007/64/CE. Ciò solleva una serie di questioni giuridiche, ad esempio sul piano della tutela dei consumatori, della sicurezza e della responsabilità nonché della concorrenza e delle questioni legate alla protezione dei dati, con particolare riguardo alla protezione dei dati degli utenti di servizi di pagamento in conformità delle norme dell'Unione sulla protezione dei dati. È quindi opportuno che le nuove disposizioni affrontino tali aspetti».

[14] Considerando 28, direttiva 2015/2366/UE: «[…] gli sviluppi tecnologici degli ultimi anni hanno portato anche alla nascita di una serie di servizi accessori, ad esempio servizi di informazione sui conti. Tali servizi forniscono all'utente di servizi di pagamento informazioni online aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce online del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento. Anche tali servizi dovrebbero essere trattati nella presente direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo status di prestatore di servizi di informazione sui conti».

strettamente collegato ai pagamenti tramite carta e, pertanto, non va considerato come servizio autonomo, bensì strumentale al prestatore di servizi di pagamento che emette lo strumento di pagamento basato su carta [15].

È evidente che i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti siano soggetti che non gestiscono il conto sul quale sono presenti i fondi dell'utilizzatore [16], che quindi restano radicati presso la banca o altro Istituto di Pagamento (ASPSP – *Account Servicing Payment Service Provider*).

Eppure, nell'ambito di questo fenomeno di disintermediazione, alla luce della complessità che caratterizza i pagamenti elettronici, appare indispensabile garantire l'utente dai rischi che simili strumenti comportano, specie sotto il profilo dell'utilizzo indebito da parte di terzi.

In effetti, la stessa PSD2 arriva in ritardo rispetto a quella che è stata l'evoluzione dei sistemi di pagamento negli ultimi anni. In altri termini, ancora una volta, la tecnologia si evolve in tempi troppo celeri rispetto a quelli necessari all'ordinamento per intervenire.

Quindi, si è posta la necessità di predisporre regole di sicurezza stringenti e, al contempo, flessibili, che siano in grado di garantire la sicurezza – dell'utente ma anche dei prestatori di servizi – e che, tuttavia, siano suscettibili di adeguarsi in modo elastico alla menzionata evoluzione delle tecniche, al fine – quantomeno – di contenere il ricorso al procedimento legislativo.

Tale bisogno, già evidenziato per la PSD, sembra essere stato preso in considerazione anche dalla PSD2 che, a tale scopo, si muove secondo una duplice prospettiva: tutela del consumatore (e, più in generale, dell'utente), anche in riferimento al trattamento dei dati [17], ed efficienza e armo-

---

[15] V. considerando 67-68, direttiva 2015/2366/UE. In proposito, V. PROFETA, *I Third Party Provider: profili soggettivi ed oggettivi*, cit., spec. p. 54, nota 11.

[16] L'art. 4, n. 17, della direttiva definisce "prestatore di servizi di pagamento di radicamento del conto" come «un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore».

[17] Sul rapporto tra PSD2 ed il regolamento (UE) 2016/679 (GDPR), V. ZENO-ZENCOVICH, *Prefazione*, cit., pp. 10-11: «La raccolta di dati è dunque essenziale per il buon funzionamento del mercato, sia per controllare in tempo reale la posizione dei soggetti, sia per valutare rischi e opportunità nelle operazioni di credito. "Know your client" non è solo uno slogan, ma un preciso obbligo. Tutto questo però collide frontalmente con la retorica della protezione dei dati personali, incarnata dal Regolamento generale sulla protezione dei dati personali (GDPR – Regolamento 679/16) che vorrebbe sottoporre l'acquisizione, la elaborazione e la circolazione dei dati personali ad un costante controllo dell'interessato, di cui la pietra di volta è il consenso e la indisponibile facoltà di revoca dello stesso, sempre, comunque e senza oneri economici o motivazionali». Cfr. 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*, cit., spec. p. 91 ss.; D. DE PAOLI, *PSD2 e Privacy*, *ivi*, p. 147 ss.;

nizzazione del mercato interno, mediante una ripartizione delle perdite subìte dall'utente per l'utilizzo fraudolento dei sistemi di pagamento [18].

Quanto appena affermato trova pieno conforto rispetto alla definizione dell'ambito di applicazione oggettivo della direttiva in esame. In particolare, nelle disposizioni relative alla predisposizione delle misure di sicurezza cui si è accennato, il legislatore comunitario si limita a fornire una serie di parametri che i prestatori di servizi di pagamento sono tenuti a rispettare. Tuttavia, la specificazione degli *standard* tecnici (cc.dd. *Regulatorytechnical standards*), anche al fine di un costante adeguamento degli stessi rispetto alle innovazioni tecnologiche – peraltro sempre con l'obiettivo di minimizzazione delle minacce alla protezione dei dati [19] –, è demandata all'Autorità Bancaria Europea, sulla scorta del regolamento (UE) n. 1093/2010 [20].

La direttiva, infatti, impone la c.d. autenticazione forte dell'utilizzatore (SCA – *Strong Customer Authentication*), cioè una procedura – diretta a verificare l'identità dell'utente e la validità dell'uso di uno specifico sistema di pagamento [21] – «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

---

C. SERTOLI, *PSD2, sicurezza e privacy*, in *Fintech: diritti, concorrenza, regole*, cit., p. 157 ss.; R. PETTI, *Identità digitale e biometria nei servizi di pagamento*, *ivi*, p. 453 ss.

[18] Cfr. il considerando 73, direttiva 2015/2366/UE, per cui: «È opportuno prevedere disposizioni per la ripartizione delle perdite in caso di operazioni di pagamento non autorizzate. Disposizioni diverse possono applicarsi agli utenti di servizi di pagamento qualora essi non siano consumatori, in quanto tali utenti sono normalmente in grado di valutare meglio il rischio di frode e di adottare contromisure al fine di garantire un livello elevato di protezione del consumatore, i pagatori dovrebbero avere sempre il diritto di chiedere il rimborso al proprio prestatore di servizi di pagamento di radicamento del conto, anche qualora un prestatore di servizi di disposizione di ordine di pagamento sia coinvolto nell'operazione di pagamento. Ciò non pregiudica la ripartizione delle responsabilità tra i prestatori di servizi di pagamento». V. anche il considerando 74, nella parte in cui dispone che «[…] una ripartizione delle responsabilità tra il prestatore di servizi di pagamento di radicamento del conto e il prestatore dei servizi di disposizione di ordine di pagamento coinvolti nell'operazione induca entrambi i soggetti ad assumersi la responsabilità per la parte dell'operazione sotto il loro controllo». In relazione agli ordini di pagamento non autorizzati ed alla conseguente allocazione di rischi e responsabilità nel PSD, v. O. TROIANO, *Contratto di pagamento*, cit., p. 409.

[19] Considerando 94, direttiva 2015/2366/UE.

[20] EUROPEAN BANKING AUTHORITY, *Final Report Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, 12 dicembre 2017; ID., *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, 21 giugno 2019. In argomento, v. anche D. GAMMALDI, *La sicurezza degli strumenti e del mercato dei pagamenti*, cit., pp. 157-159.

[21] Cfr. art. 4, n. 29, direttiva 2015/2366/UE.

non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione»[22].

La previsione di un sistema di sicurezza fondato sull'autenticazione forte – si è detto – va letta nel senso di ridurre il rischio di operazioni non autorizzate mediante lo strumento di pagamento dell'utente – salvi, naturalmente, i casi di comportamenti fraudolenti dell'utente stesso –e di determinare, al contempo, una diversa allocazione della responsabilità e del rischio in base alle differenti tipologie dei servizi prestati.

D'altronde, sebbene in termini meno stringenti, un sistema di autenticazione dell'utente era già previsto nella PSD.

L'abrogata disciplina, sempre in un'ottica di *favor* dell'utente/consumatore, imponeva a carico dell'utente di servizi di pagamento alcuni obblighi che, in buona sostanza, costituivano espressione di un dovere di comportamento conforme ai doveri di buona fede e di diligenza nell'esecuzione del contratto (basti pensare ai doveri di custodia delle credenziali della carta). Dall'altro lato, gravavano sul prestatore di servizi una serie di obblighi ulteriori, ricollegati alla natura stessa dell'attività prestata ed al rischio d'impresa che caratterizza il mercato dei servizi di pagamento[23].

L'attuale quadro normativo implementa il *favor* accordato in precedenza al consumatore/utente, atteso che in tal modo si pone a carico del prestatore l'onere di predisporre le misure idonee a prevenire il rischio di operazioni di pagamento non autorizzate.

Ed è proprio da questa prospettiva che va letta la disposizione di cui all'art. 72 della PDS2 che impone al prestatore di servizi di fornire non soltanto «la prova del fatto che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti del servizio fornito» ma, altresì, «gli elementi di prova che dimostrano la frode o la negligenza grave da parte dell'utente di servizi di pagamento».

Quanto finora descritto spiega anche la riduzione della franchigia – e, quindi, del massimo importo che il pagatore è tenuto a sopportare in caso di operazioni non autorizzate – a 50 euro, mentre la PSD stabiliva un importo non superiore ad euro 150[24].

---

[22] Art. 4, n. 30, direttiva 2015/2366/UE. In proposito, si veda anche EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, p. 4 ss.

[23] Cfr., in particolare, artt. 56 e 57, direttiva 2007/64/CE. V. anche O. TROIANO, *Contratto di pagamento*, cit., spec. pp. 407-413.

[24] V. art. 74, direttiva 2015/2366/UE e art. 61, direttiva 2007/64/CE.

3. La tutela dell'utente nell'ordinamento italiano: profili applicativi nella giurisprudenza dell'Arbitro Bancario Finanziario

Si è detto che, per quanto riguarda l'ordinamento italiano, la PSD2 è stata recepita mediante il d.lgs. n. 218/2017, che ha modificato una serie di disposizioni contenute nella normativa di recepimento della PSD, cioè il d.lgs. n. 11/2010[25].

In riferimento al tema dell'autenticazione fin qui analizzato, ai sensi dell'art. 12, comma 2-*bis*, d.lgs. n. 11/2010, «salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente».

Inoltre, il novellato art. 12 prevede, al comma 3, che «il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita».

Sempre in merito al *favor* nei confronti del cliente, va sottolineato che l'ultimo capoverso dell'art. 10, d.lgs. n. 11/2010, così come modificato dal citato d.lgs. n. 218/2017, dispone che è onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente, al fine di far ricadere su quest'ultimo i costi dell'operazione non autorizzata.

Peraltro, l'attuale formulazione dell'art. 11 non si limita più a prevedere genericamente l'obbligo del rimborso bensì impone tempi certi entro i quali esso deve avvenire[26].

La norma, infatti, prevede espressamente che «[…] il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito».

Tuttavia, analizzando la corposa giurisprudenza dell'Arbitro Bancario Finanziario in materia, si evince agevolmente che, nella maggior parte dei casi, i prestatori di servizi di pagamento tendono a non rimborsare imme-

---

[25] S. VANINI, *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218*, in *Nuove leggi civ. comm.*, 2018, p. 866 ss.

[26] Sull'obbligo di rimborso, v. V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè, Milano, 2016, p. 169 ss.; ID., *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, cit., p. 31 ss.

diatamente l'importo, ma, anzi, a ritenere legittime le operazioni contestate dagli utenti, spesso prospettando la loro negligenza rispetto agli obblighi di custodia e di conservazione degli strumenti di pagamento e delle credenziali (tanto di quelle statiche, quanto di quelle dinamiche) [27].

Ebbene, in riferimento a tale ultimo profilo, sempre tenendo ben presente il *favor* suddetto, nel considerando 72 della PSD2, il legislatore europeo afferma che «il concetto di negligenza implica la violazione del dovere di diligenza, mentre per negligenza grave si dovrebbe intendere un comportamento che si spinge oltre la semplice negligenza e implica un grado significativo di mancanza di diligenza […] I termini e le condizioni contrattuali per la fornitura e l'uso di uno strumento di pagamento, il cui effetto sarebbe quello di aumentare l'onere della prova per il consumatore o ridurre l'onere della prova per l'emittente, andrebbero considerate nulle e prive di effetti. Inoltre, in situazioni specifiche, in particolare se lo strumento di pagamento non è utilizzato presso il punto vendita, come nel caso dei pagamenti online, è opportuno che il prestatore di servizi di pagamento sia tenuto a fornire prove della presunta negligenza poiché in tali casi i mezzi a disposizione del pagatore sono molto limitati».

È interessante notare come l'Arbitro Bancario Finanziario [28], nelle ipotesi di utilizzo non autorizzato sottoposte alla sua attenzione, abbia sempre posto l'accento sui doveri di diligenza e buona fede di entrambe le parti del rapporto in esame [29]. In effetti, le pronunce dell'Arbitro muovono sempre dalla prospettiva di valutare con estrema attenzione non soltanto il rispetto degli obblighi di diligente custodia e conservazione degli strumenti di pagamento posti a carico dell'utente [30], ma anche – e soprattutto – di

[27] Ad ogni modo, nell'esperienza dell'Arbitro, non mancano ipotesi in cui si pone in evidenza il comportamento gravemente negligente dell'utilizzatore che può determinare o una ripartizione delle responsabilità – e, quindi, un concorso di colpa *ex* art. 1227 c.c. (cfr. ABF – Collegio di Napoli, decisione n. 15000/2018) – oppure una decisione di non accoglimento del ricorso del ricorrente (cfr. ABF – Collegio di Napoli, decisione n. 13004/2019).

[28] Sul funzionamento dell'Arbitro Bancario Finanziario si rinvia a G.L. CARRIERO, *L'Arbitro Bancario Finanziario presso la Banca d'Italia: genesi, struttura e funzioni*, in *Trattato di Diritto dell'Arbitrato*, diretto da D. MANTUCCI, ESI, Napoli, 2020, p. 1 ss. Per una prospettiva comparata, si rinvia a S. SICA, C. TROISI, V. CARRIERO, *Gli arbitrati bancari e finanziari nelle esperienze straniere*, *ivi*, p. 519 ss.

[29] In relazione alle ipotesi di *phishing* nella giurisprudenza ordinaria ed arbitrale, B. RUSSO, *I nuovi orientamenti giurisprudenziali sul reato di phishing: "la banca è responsabile se non prova che il cliente ha disposto il pagamento"*, in *Riv. dir. banc.*, 2019, IV, p. 71 ss.

[30] Sulla definizione di colpa grave dell'utilizzatore, v. ABF – Collegio di Coordinamento, decisione n. 6168/2013, in cui il Collegio, mutuando anche dalla giurisprudenza della Suprema Corte di Cassazione, afferma che essa debba intendersi come «un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o

quelli imposti al prestatore di servizi di pagamento, attesa la diligenza professionale *ex* art. 1176, comma 2, c.c., facendo ricadere su quest'ultimo un vero e proprio rischio d'impresa[31].

A dimostrazione di quanto affermato, va evidenziato che già con decisione n. 3498/2012 – e quindi sotto la vigenza della PSD – il Collegio di Coordinamento, in un caso di *man in the browser*, ha affermato che «lo squilibrio di responsabilità promanante dal dettato normativo del d.lgs. 11/2010, si spiega in considerazione dell'incomparabilmente maggior capacità economica dell'intermediario di sostenere il rischio connesso all'impiego di strumenti la cui sicurezza assoluta non è stata sin qui raggiunta (e probabilmente non verrà mai raggiunta dato l'inarrestabile evolversi della tecnologia civile e la naturale "rincorsa" della tecnologia criminale

---

negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti».

[31] Al riguardo, v. I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. n. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ.*, 2016, p. 471: «Nel settore dei servizi di pagamento, tuttavia, la "pericolosità" dell'attività svolta che interessa una vasta platea di consumatori o di utenti, sembra aver indotto il legislatore ad ampliare l'ambito del rischio d'impresa, facendo gravare i pericoli di danno statisticamente prevedibili legati all'esercizio sull'impresa stessa, in quanto quest'ultima è l'unica in grado di distribuire il rischio dell'impiego di strumenti di pagamento»; V. PROFETA, *I Third Party Provider*, cit., p. 75: «La PSD2, dunque, non soltanto conferma in generale la linea inaugurata dalla PSD1 di ampliare l'ambito del rischio di impresa in capo al prestatore di servizi di pagamento, gravandolo dei pericoli di danno statisticamente prevedibili in relazione allo svolgimento di tale attività, con la finalità di promuovere negli utenti la fiducia nell'utilizzo degli strumenti di pagamento elettronici, ma va oltre, introducendo un obbligo di rimborso in capo al prestatore di radicamento del conto a prescindere dalla sua responsabilità nella causazione dell'illecito pagamento e spostando in capo al TPP che ha disposto l'ordine di pagamento la presunzione di responsabilità nella successiva regolazione dei rapporti tra gli intermediari coinvolti nell'operazione di pagamento contestata».

Nella giurisprudenza arbitrale, è stato sottolineato che la disciplina europea degli strumenti di pagamento è «evidentemente ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a "spalmare" sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore, in funzione dell'obiettivo di incrementare la fiducia del pubblico riguardo ai suddetti strumenti e di incentivarne l'uso e la diffusione, in quanto strumenti atti a facilitare e perciò a moltiplicare le transazioni commerciali, nell'interesse delle imprese, degli stessi utenti/consumatori, nonché, ovviamente, delle banche» (ABF – Collegio di Roma, decisione n. 1111/2010). Inoltre, nell'ambito del vasto panorama giurisprudenziale dell'Arbitro, si rinvia a mero titolo esemplificativo, a Collegio di Coordinamento, decisioni n. 3947/2014, n. 991/2014 e n. 3498/2012; nonché a Collegio di Napoli, decisione 4754/2018, e Collegio di Bari, decisione n. 3686/2019.

nella stessa direzione), grazie ad una redistribuzione dei relativi costi sull'intero pubblico dell'utenza»[32].

Infatti, di là dai casi in cui il cliente abbia evidentemente fornito a terzi le proprie credenziali (e, segnatamente, i codici OTP), le decisioni dell'Arbitro tendono a considerare lo squilibrio che informa il rapporto tra le due parti; per tali motivi, nella giurisprudenza arbitrale è stato più volte ribadito il principio per il quale la mera dimostrazione documentale che l'autenticazione è stata effettuata con le credenziali dell'utente non libera, di per sé sola, l'intermediario dalle proprie responsabilità.

Il prestatore di servizi, infatti, adotta tecnologie in grado di rilevare indici di anomalia all'interno dell'attività del singolo strumento di pagamento, tali da allertare il prestatore, anche sulla scorta della c.d. normativa "anti-frode"[33].

A mero titolo esemplificativo, basti pensare a tutti i casi in cui le operazioni si susseguono troppo velocemente in un lasso temporale breve; oppure l'indirizzo IP da cui le operazioni sono disposte non è mai apparso nella storia dell'utente e l'importo complessivo supera il *plafond* contrattualmente previsto[34].

Invero, ai sensi dell'art. 10, d.lgs. n. 11/2010, così come novellato dalla PSD2, qualora l'utente neghi di avere autorizzato un'operazione di pagamento, il prestatore di servizi ha l'onere di fornire prova che: l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti». Peraltro, ai sensi

---

[32] Cfr. anche ABF – Collegio di Napoli, decisione n. 9080/2017, e Collegio di Roma, decisione n. 1179/2017.

[33] Il riferimento è alla legge 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento» e all'art. 8 del Decreto del Ministero dell'Economia e delle Finanze del 30 aprile 2007, n. 112 che fornisce l'elenco dei casi in cui il rischio frode si configura. Il comportamento omissivo dell'intermediario rispetto agli obblighi di monitoraggio di operazioni sospette e di attivazione dei presidii di sicurezza è stato oggetto di censura da parte di ABF – Collegio di Roma, decisione n. 8569/2016, con commento di R. MARSEGLIA, *La responsabilità da* status *della banca in caso di clonazione della carta prepagata*, in *Giur. it*., 12, 2017, p. 2632 ss.

[34] Cfr. ABF – Collegio di Coordinamento, decisione n. 16237/2018, nella parte in cui afferma che «l'importo dell'operazione disposta fraudolentemente con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. *plafond*) per l'utilizzo dello strumento elettronico di pagamento deve essere quindi interamente restituita al cliente e ciò in quanto difetta del suo consenso risultando difforme alle limitazioni contrattuali di operatività dello stesso. In tali casi la condotta dell'intermediario concreta la violazione delle norme pattizie poste quali obblighi di protezione gravanti sui prestatori di servizi di pagamento in ragione di un'interpretazione costituzionalmente orientata del combinato disposto degli artt. 1175 e 1375 c.c.».

dell'ultimo inciso del comma 3 della citata disposizione, «è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente».

Al riguardo, il Collegio di Coordinamento (decisione n. 22745/2019), anche sulla scorta dell'orientamento dei Collegi territoriali, ha rilevato che, «l'onere probatorio previsto nei commi 1 e 2 dell'art. 10 del decreto deve necessariamente essere assolto dal PSP con riguardo ad ambedue i profili (autenticazione ed esecuzione delle operazioni di pagamento, nonché colpa grave dell'utilizzatore), da ritenersi necessari e complementari. Pertanto, […] il Collegio giudicante non potrebbe desumere la sussistenza della frode, del dolo o della colpa grave dell'utente soltanto dalla prova della "regolarità formale" dell'operazione. Ne consegue che, nel caso in cui l'intermediario si limiti a produrre semplicemente il "log informatico" relativo all'operazione contestata, senza altra allegazione diretta a comprovare, in via presuntiva, l'apporto causale del ricorrente nel compimento dell'operazione stessa, senza condizionamenti, interferenze, deviazioni, hacker o altre anomalie risultanti dai sistemi antifrode o comunque dai dati conoscitivi in suo possesso, il Collegio dovrà ritenere non assolto l'onere probatorio ai sensi dell'art. 10, comma 2 del decreto e conseguentemente accogliere il ricorso»[35].

Proprio in riferimento all'esclusione della colpa grave dell'utilizzatore, sono interessanti le considerazioni espresse dal Collegio di Napoli, nella decisione n. 22389/2019, in relazione ad un caso di *software* installato tramite raggiri sofisticati.

In tal caso, l'Arbitro ha rilevato che «la ricostruzione dell'operazione contestata che emerge dagli atti del procedimento evidenzia, con alto grado di probabilità, come parte attrice sia stata vittima di un *software* malevolo, tipologia di frode sofisticata compiutamente descritta da Coll. Coord., n. 3498/2012, alle cui conclusioni questo Collegio ritiene di aderire». Ed infatti, ha accolto il ricorso, evidenziando che il comportamento delle ricorrenti non poteva essere qualificabile in termini di colpa grave.

D'altronde, sempre in relazione all'analisi del comportamento delle parti, non è insolito che l'Arbitro Bancario Finanziario rilevi una responsabilità dell'intermediario per la mancata attivazione del servizio di *sms alert*, talvolta ripartendo in misura equitativa le perdite tra utente e prestatore,

---

[35] V. ABF – Collegio di Coordinamento, decisioni nn. 10929/2016 e 7716/2017. In riferimento all'onere della prova nell'ambito del procedimento dinanzi all'Arbitro, v. D. DALFINO, *L'Abf e i principi del processo civile: contestazione, "contumacia", onere della prova*, in *Il Processo*, 1, 2019, p. 27 ss.

altre volte facendo ricadere soltanto su quest'ultimo l'intero importo delle operazioni fraudolente effettuate proprio a causa del contegno omissivo. Ciò purché sia rilevato il nesso causale tra la mancata attivazione del servizio ed il verificarsi del danno [36].

Al riguardo, recentemente, il Collegio di Coordinamento dell'Arbitro si è uniformato all'ormai granitico orientamento dei Collegi territoriali sul punto, per cui «la mancata attivazione del servizio di *sms alert* costituisce, come ormai è opinione consolidata di questo arbitro, una carenza organizzativa imputabile all'intermediario resistente il quale, data la natura di misura di sicurezza del sistema di *sms alert*, non dovrebbe limitarsi a proporlo al cliente ma dovrebbe adottarlo in modo generalizzato».

Infatti, con la decisione n. 24366/2019, il Coll. Coord. ha stabilito che «fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di *sms alert* o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di *alert* dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto».

In relazione al servizio di *alert* menzionato, va comunque sottolineato che non è configurabile la responsabilità dell'intermediario qualora sia stato lo stesso cliente a rifiutarne l'attivazione, mediante dichiarazione espressa e documentata [37].

Quindi, dapprima con la PSD e, poi, con la PSD2, la disciplina dei servizi di pagamento ha trovato terreno fertile nell'ambito della giurisprudenza dell'Arbitro Bancario Finanziario che, a ben vedere, ha sempre dimostrato di interpretare la normativa di riferimento in maniera attenta, avendo riguardo all'evoluzione dei rischi connessi agli strumenti elettronici di pagamento (*phishing*, clonazione, *sim swap*, ecc.), nonché al rapporto tra utilizzatore e prestatore, caratterizzato da un'evidente asimmetria.

L'analisi dell'orientamento dell'Arbitro in materia consente di porre in evidenza due elementi: in primo luogo va sottolineata la sua capacità di intervenire in modo incisivo in ordine all'adeguatezza dei sistemi di sicurezza predisposti dai diversi prestatori. Per altro verso, tale capacità si dispiega anche sul comportamento dell'utenza – il cui comportamento, pertanto, non è affatto valutato in maniera acritica in ragione del *favor* accordatogli – , attraverso l'indicazione di canoni di comportamento idonei a prevenire il rischio frode.

---

[36] Sul servizio di *sms alert*, v. anche M.C. PAGLIETTI, *Questioni in materia di prova di pagamenti non autorizzati*, cit., pp. 69-70.

[37] Cfr. ABF – Collegio di Coordinamento, decisione n. 24366/2019.

4. Riflessioni di sintesi

In definitiva, il tema in esame consente alcune considerazioni, invero, per niente "conclusive" (e non potrebbero esserlo quando c'è di mezzo il rapporto tra *LawandTech*).

Il settore dei pagamenti elettronici è riflesso, infatti, proprio del più generale "confronto" tra disciplina giuridica ed evoluzione tecnologica, alla ricerca perenne di un approccio equilibrato.

È noto che va rifuggita la tentazione del rifiuto della novità tecnologica, che, del resto, per l'evidenza dei fatti, sarebbe destinato alla frustrazione; ma occorre guardarsi anche da quella opposta, della fiducia cieca o illimitata nella capacità del sistema degli scambi di autolimitarsi, darsi regole o, addirittura, avere una dimensione etica [38].

È necessario, all'opposto, prendere atto che la "disintermediazione" è il frutto più maturo (che rischia di essere avvelenato) di un processo che ha origini ormai risalenti, che muove dalla teorica della postmodernità, passa per la globalizzazione ed oggi perviene alla pretesa della società "desoggettivizzata", profilo di estremo interesse e rischio, quanto all'A.I. [39].

Forse più che al *balance of interests*, bisogna tendere al realismo della lettura.

Il Diritto, con la D maiuscola, ovvero la capacità degli ordinamenti di comporre sintesi tra valori ed interessi, spesso o sempre conflittuali, deve recuperare terreno, ma l'obiettivo non è facile da conseguire. L'alluvione

---

[38] Sul punto, sia consentito il rinvio a S. SICA, G. GIANNONE CODIGLIONE, *La libertà fragile. Pubblico e privato al tempo della rete*, ESI, Napoli, 2014, p. 54, nella parte in cui, in riferimento al complesso rapporto tra capitalismo e libertà, si sottolinea che «vi è una dimensione del tema che attiene alla rottura dell'endiadi "libertà di impresa – garanzia di progresso sociale"; ve n'è un'altra che, dopo il primo livello di approfondimento, relativo ai poteri statali sempre più deboli eppure sempre più, a tratti, "illiberali", deve pervenire al cuore della questione senza timori e infingimenti: senza l'apparato valoriale che ne giustificava ideologicamente il fondamento, con le istituzioni della tradizione liberale ogni giorno più in difficoltà, sul versante normativo, dell'equilibrio dei poteri, dell'affermazione della sovranità consolidata, l'attività di impresa aspira all'autoreferenzialità, la coltiva come un valore; le multinazionali si sentono "autosufficienti" nella giustificazione della propria esistenza, degli accordi reciproci, delle battaglie incrociate, con la *competition*, anzi, che diventa essa stessa, al contempo, valore, criterio di selezione e perfino garanzia per i cittadini».

[39] In riferimento all'utilizzo dell'intelligenza artificiale nel settore bancario, v.: M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, cit.; G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, cit.; D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, J.N. BARBERIS, *From Fintech to TechFin: The Regulatory Challenges of Data-Driven Finance*, in *European Banking Institute Working Paper Series*, 6, 2017, reperibile al link www.ebi-europa.eu; IDD., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in *European Banking Institute Working Paper Series*, 11, 2017.

regolamentare nel campo di incrocio tra *Law and Tech* sovente impedisce la visione d'insieme, atteso che le fonti, il più delle volte, ovviamente, sovranazionali, rincorrono l'emergenza o la novità che l'impulso tecnologico propone.

L'argomento affrontato ne è una significativa esemplificazione. Se è inutile e dannoso (in una visione giuseconomica e culturale) provare a bloccare le trasformazioni e, si badi, le nuove opportunità, che la risorsa *tech* offre, è altrettanto inaccettabile relegare l'ordinamento giuridico a spettatore o, al più, fotografo della realtà.

La risposta che la PSD2 propone sembra muoversi nella descritta (equilibrata) prospettiva. Tuttavia, mai come ora, è fondamentale l'implementazione che della regola legislativa effettua la giurisprudenza. In particolare, di estremo interesse, anche sul versante sistematico, è parso l'intervento dell'Arbitro Bancario Finanziario che, per come si è visto, risulta improntato, appunto, ad un sano realismo, esemplificativo della necessaria ricerca di "sforzi" del Diritto nelle pieghe delle "regole" [40].

Che cosa palesa, in ultima analisi, l'orientamento dell'Arbitro? La disintermediazione, e, vieppiù, la spersonalizzazione della relazione tra banca (intermediario?) e cliente offre enormi opportunità di espansione dei traffici, che non possono né debbono essere smarrite.

Il primo beneficiario delle novità è certamente il sistema bancario e finanziario ed è pertanto giusto che su di esso vada primariamente allocato il rischio di malfunzionamento o di un uso abusivo del modello tecnologico; il che è percepibile in primo luogo con riguardo alla distribuzione dell'onere probatorio [41].

Ma vi è anche la consapevolezza che, in un contesto globalizzato e disintermediato, la stessa idea di "forza" dell'imprenditore (bancario/finanziario) va ripensata. E probabilmente si impone una riflessione sull'utente del servizio disintermediato: certamente è più esposto e, dunque, debole, ma gli si richiede uno sforzo di crescita culturale. Se egli, si è visto, non tiene condotte collaborative e, ad esempio, rifiuta l'attivazione di meccanismi di *alert*, è giusto riallocare nella sua sfera, in tutto o in parte, i collegati rischi e danni [42].

In definitiva, la questione nodale diventa la gestione della "patologia"

---

[40]Il riferimento è, in particolare, a ABF – Collegio di Coordinamento, decisione n. 22745/2019.

[41]Nello stesso senso si muove la Corte di Cassazione. Cfr. Cass., 12 aprile 2018, n. 9158; Cass., 3 febbraio 2017, n. 2950; Cass., 12 giugno 2007, n. 13777.

[42]V. anche ABF – Collegio di Coordinamento, decisione nn. 8553/2019, e Collegio di Palermo, decisione n. 13205/2017.

del fenomeno della disintermediazione; come si è avuto modo di sottolineare in relazione ad altri ambiti di intersezione tra diritto e tecnologie – si pensi, su tutti, al tema della responsabilità civile da trattamento illecito dei dati personali [43] – è velleitaria l'idea dell'esclusione del rischio, che viceversa diventa la cifra identificativa dello sviluppo tecnologico. Il che comporta che si abbandonino prospettive forse plausibili o teoricamente "perfette" in linea concettuale ed in generale, ma inammissibili ove il campo di applicazione abbia come paradigma l'espansione massima della potenzialità applicativa. Più chiaramente, se la possibilità tecnologica diventa effettiva, probabilmente il diritto è già in ritardo e deve fare i conti con la capacità di governo del fenomeno soprattutto in sede rimediale.

Ed allora il quesito da porsi è se, di là dall'impianto complessivo, la disciplina di PSD2, per quanto già emerso in sede giurisprudenziale e nel momento interpretativo, riesca a far fronte alla prevalente (se non esclusiva) esigenza di corretta ed equilibrata *risk allocation*, nella consapevolezza dell'ineliminabilità in sé del rischio connesso alle nuove figure di pagamento ed ai nuovi *players* del settore [44].

D'altro canto, è pur vero che l'unico modello di ricostruzione della vicenda non può che fare i conti con la standardizzazione – che è profilo tecnico – dei livelli esigibili di sicurezza dei pagamenti.

In realtà, il vero snodo è proprio l'allocazione del rischio e di questo ha mostrato consapevolezza sia il legislatore europeo che quello interno; ma il punto è come garantire i molteplici interessi in gioco: fiducia degli utenti sull'affidabilità del sistema, garanzia di alti standard di sicurezza, prevenzione di comportamenti negligenti o de-responsabilizzati degli utenti stessi.

Il che equivale ad interrogarsi, in ultima analisi, sul criterio più efficiente di imputazione della responsabilità per violazione o uso improprio o *default* del sistema. Nel complesso può tranquillamente affermarsi che il territorio della responsabilità per colpa in materia pare davvero residuale; è corretto, viceversa, sostenere che nell'impianto della direttiva è data prefe-

---

[43] Sia consentito il rinvio a S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di A. Mantelero, D. Poletti, Pisa University Press, 2018, pp. 161-174.

[44] È stato giustamente osservato da M.C. PAGLIETTI, *Questioni in materia di prova di pagamenti non autorizzati*, cit., p. 55, che «il tema della sicurezza, uno dei pilastri tanto della prima quanto della seconda versione della normativa che occupa, viene svolto sulla base dell'assunto che, in materia, è impossibile raggiungere la totale invulnerabilità di un sistema per un periodo prolungato; posto dunque che un margine di rischio è ineliminabile, accorgimenti vengono imposti allo scopo di «mitigare» il rischio, non eliminarlo».

renza al caricamento del rischio al prestatore; si pensi all'art. 12, d.lgs. n. 11/2010, che contempla un alternativo regime di responsabilità dell'utente, limitata e illimitata. La prima si configura in relazione ad operazioni poste in essere prima della tempestiva comunicazione di cui all'art. 7, nei limiti della franchigia, ora ridotta ad euro 50 (art. 12, comma 3) [45].

La responsabilità illimitata dell'utente, invece, si configura qualora egli abbia agito in modo fraudolento, con dolo o colpa grave, contravvenendo ai propri obblighi di custodia delle credenziali e dello strumento di pagamento (art. 7, comma 1, lett. a, e comma 3); ovvero se non abbia dato tempestiva comunicazione dello smarrimento, furto, appropriazione indebita dello stesso (art. 7, comma 1, lett. b). Ma tale apertura ad una responsabilizzazione dell'utente è immediatamente mitigata nei casi di mancata adozione del prescritto sistema di autenticazione multi-fattore: la responsabilità dell'utente, viene esclusa anche nell'ipotesi di una sua condotta caratterizzata da dolo o colpa grave, ed è ravvisabile nel solo caso di frode dello stesso (la cui prova è a carico del prestatore: art. 12, comma 2-*bis*). Tra l'altro, come è stato opportunamente sottolineato, il fondamento di siffatta responsabilità sembra più sanzionatorio che restitutorio [46].

Nell'insieme è fondato sostenere che il modello legislativo è ispirato ad una responsabilità "oggettiva", come principio generale. Ma la vera novità è probabilmente da scorgere nella presa d'atto da parte del legislatore che ormai si è intrapreso un cammino in parte ignoto: ne è riprova l'art. 10, comma 1-*bis*, che contempla l'ipotesi del danno generato da causa sconosciuta; insomma è chiara l'idea della instabilità per definizione dell'assetto raggiunto, che impone una necessaria verifica del mutamento dello scenario tecnologico e delle falle del sistema che aprano la strada a nuovi utilizzi fraudolenti.

Il passaggio da autenticazione forte monofattore a multifattore, che la PSD2 introduce, a quale logica è riconducibile? Comporta un mutamento del criterio interpretativo dell'intera disciplina del settore? Probabilmente la risposta è negativa. Il dettaglio analitico del legislatore per esempio nel riparto di compiti (e di responsabilità) dei vari *players* – si pensi all'art. 11

---

[45] In questi termini si esprime M.C. PAGLIETTI, *Questioni in materia di prova di pagamenti non autorizzati*, cit., p. 50.

[46] Cfr. M.C. PAGLIETTI, *Questioni in materia di prova di pagamenti non autorizzati*, cit., p. 51. L'A., inoltre, pone l'accento sui cc.dd. danni da ignoto tecnologico e sottolinea che «in tema di allocazione delle responsabilità, va inoltre tenuta in debita considerazione la prospettiva della probabile evoluzione dei fatti fraudolenti nuovi, ossia fatti generatori di responsabilità riconducibili alle ipotesi di danno da ignoto tecnologico (il danno, cioè, verificatosi a causa di una causa sconosciuta, quali possono essere considerati gli «inconvenienti» menzionati dall'art. 10, comma 1-*bis*), dei quali viene gravata l'impresa».

del d.lgs. n. 11 – non deve indurre in inganno: la sostanziale solidarietà nei confronti degli utenti semmai conferma che siamo innanzi ad un'ipotesi di rischio di impresa, quanto alla rilevanza esterna. Semmai il punto è come collegare l'incremento della sicurezza dell'autenticazione con il tradizionale campo della diligenza esigibile, in particolare *ex* art. 1176, comma 2, c.c.

Inoltre, v'è da chiedersi, se si pensa all'orientamento innanzi esaminato dell'ABF, quanto esso mantenga attualità e possa dirsi efficiente nell'ottica della PSD2.

Ovvio che l'intera riflessione si sposta nel difficile territorio dell'onere della prova, dove non è sufficiente constatare la scelta legislativa per un meccanismo di inversione a carico del o dei prestatori; fin qui siamo di fronte alla consolidata *policy* degli ordinamenti europei rispetto ai rischi socialmente rilevanti (il pensiero va, in primo luogo, all'art. 2054 e soprattutto 2050 del nostro codice civile) [47]. Né può dirsi esaustivo prendere atto che il legislatore richieda che sia comunque il prestatore a dimostrare la colpa grave "assorbente" dell'utente.

Se c'è un istituto in cui la struttura risente dell'incidenza del profilo funzionale, questo è la responsabilità (sia aquiliana che contrattuale); sicché non è sufficiente ragionare in termini di inversione dell'onere della prova. Si pensi al *phishing*: esso talora presenta fattezze che il consumatore medio "non può non riconoscere" ed è corretto addossare allo stesso le conseguenze del proprio incauto comportamento. Ma è impossibile ricavarne una regola generale, nel senso che talora lo stesso fenomeno si determina in un contesto spazio-temporale peculiare (è il caso del c.d. *real time phishing*) che preclude all'utente di percepire l'inganno in cui sta cadendo.

Insomma, nella variabilità e "precarietà" della morfologia delle situazioni e delle combinazioni di fattori tecnici, le sole regole di principio ricavabili, paiono le seguenti:

– la disciplina manifesta (*rectius*, conferma) l'inevitabile *favor* per l'utente, nella logica propria dei rapporti asimmetrici, di consolidata esperienza europea;

– la pluralità di *players* non è senza significato ma assume essenzialmente rilievo nel *partage* di responsabilità tra i medesimi;

– l'intero impianto è connotato dall'aspirazione alla riduzione del rischio, ma nella consapevolezza che va gestita la patologia (a tratti) inevitabile del sistema;

---

[47] Sul punto, v. anche V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, cit., p. 25 ss.

– l'utente è tuttavia chiamato ad una crescita di consapevolezza nell'utilizzo delle nuove opportunità tecnologiche, anche per le potenziali (comunque circoscritte) ricadute delle proprie condotte sul versante dell'esonero da responsabilità dei prestatori [48].

Insomma, da un ambito di nicchia, sebbene fortemente pervasivo dell'economia globale, può derivare una seria prospettiva di lavoro per riconciliare Diritto e tecnologia e, se si vuole, capitalismo finanziario e prerogative valoriali In tale dimensione ciascuno – giudice e interprete soprattutto – deve rinunziare ad alcune certezze monolitiche, accettando la linea della flessibilità di approccio; il che non impedisce al Diritto di dettare la via preferita, che, fino a prova contraria, oggi è quella dell'espansione dell'economia digitale de-soggettivizzata, cui fa da contrappeso la tutela prioritaria degli utenti "in carne ed ossa".

[48] Cfr., in particolare, M.C. PAGLIETTI, M.I. VANGELISTI (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, cit., *passim*; G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Zanichelli, Torino, 2019, *passim*; F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, in Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019, *passim.*