BANCA D'ITALIA
EUROSISTEMA

Il diritto nell'era dei pagamenti digitali: le condizioni per un mercato competitivo

Intervento di Chiara Scotti
Vice Direttrice generale della Banca d'Italia[1]

Discorso in occasione della conferenza "Contratto e Concorrenza nel Mercato Bancario. Europa e Competitività"

Palermo, 12 novembre 2026

Contratto e concorrenza sono due elementi essenziali del funzionamento del mercato. Il contratto regola i rapporti tra le parti; la concorrenza determina il contesto nel quale quei rapporti si formano, definendo le alternative disponibili e le condizioni dello scambio. L'innovazione tecnologica sta incidendo su entrambi, anche in campo finanziario, modificando la struttura dei mercati, le relazioni tra gli operatori e le condizioni in cui imprese e consumatori esercitano la propria libertà contrattuale. Ne derivano questioni rilevanti per il diritto e per la regolazione.

Vorrei affrontare questo tema partendo dal mondo dei pagamenti, nel quale emergono con particolare evidenza alcune delle trasformazioni più significative innescate dall'innovazione tecnologica. Un pagamento digitale, infatti, è sempre meno riconducibile alla sola esecuzione di un ordine di trasferimento di fondi dato dal cliente al proprio intermediario. Spesso è invece il risultato di una filiera articolata: nell'acquisto tramite smartphone di un abbonamento a un servizio di musica in *streaming*, ad esempio, oltre al cliente e alla sua banca possono intervenire il produttore del dispositivo, il gestore dello schema di pagamento e quello della piattaforma sottostante all'app store e al sistema operativo, nonché diversi fornitori tecnologici[2]. Con lo sviluppo dell'intelligenza artificiale agentica anche la ricerca dei beni e servizi da acquistare e l'esecuzione del pagamento possono essere delegate a sistemi capaci di operare per conto dell'utente.

Il pagamento resta quindi un elemento chiave del rapporto contrattuale, ma il suo funzionamento dipende sempre più dall'interazione di una pluralità di operatori.

---

1 Ringrazio Claudia Biancotti e Oscar Borgogno per il supporto che hanno fornito nella preparazione di questo intervento.

2 Nell'esempio citato interagiscono, oltre al pagatore e alla sua banca, il produttore dello smartphone (il cui *secure element* conserva i dati della carta tokenizzata), il gestore dello schema di carte, il gestore del *gateway* di pagamento, la piattaforma digitale che eroga il servizio e i fornitori di servizi tecnologici e di connettività che assicurano l'identificazione dei soggetti, la trasmissione sicura dei dati e la concatenazione in tempo reale delle fasi.

Questo nuovo assetto modifica anche le condizioni di concorrenza. Una parte crescente della capacità di offrire un servizio dipende dalla possibilità di accedere alle infrastrutture, ai dati, alle interfacce e agli algoritmi che costituiscono lo scheletro del mercato.

Nell'ultimo decennio il quadro normativo europeo in materia bancaria, finanziaria e di concorrenza ha perciò affiancato ai tradizionali strumenti di correzione *ex post* una più marcata dimensione regolatoria *ex ante*, volta a preservare l'accesso e la contendibilità dei mercati, affrontando le problematiche derivanti dai colli di bottiglia tecnologici.

In questo quadro emergono, a mio avviso, tre questioni fondamentali per il diritto.

Chi risponde? Come allocare le responsabilità quando la posizione contrattuale degli operatori coinvolti non coincide con quella di chi dispone concretamente delle informazioni e degli strumenti per prevenire il rischio?

Come garantire l'accesso al mercato? Come e quando intervenire quando infrastrutture essenziali per la concorrenza, come dati, interfacce e standard tecnologici, sono controllate da soggetti privati?

Che cosa sostiene la fiducia nel mercato dei servizi di pagamento? Oltre all'affidabilità dei dati e alla resilienza delle infrastrutture, quali caratteristiche deve avere il quadro giuridico perché il mercato funzioni in modo sicuro e resiliente?

È attraverso queste tre domande che vorrei guardare all'evoluzione del mercato europeo dei pagamenti e, più in generale, al ruolo del diritto nel definire le condizioni per un ecosistema digitale competitivo, innovativo e attento alla tutela degli utenti. Si tratta di questioni complesse, che non ammettono risposte immediate o definitive, ma che ritengo utile portare alla vostra attenzione per alimentare il confronto nel corso della conferenza.

1. Chi risponde? Dal contratto alla filiera

La maggiore articolazione e complessità della filiera dei pagamenti incide sull'attribuzione delle responsabilità: un tema giuridico che va affrontato per evitare ripercussioni negative in primo luogo sugli utenti.

A questo si aggiunge la grande rapidità di esecuzione. Nei pagamenti istantanei, in particolare, il tempo per intervenire in caso di errore o frode è minimo e gli interventi correttivi successivi risultano spesso complessi e onerosi, anche per la necessità di allocare perdite tra operatori e utenti. Una parte fondamentale della protezione deve quindi spostarsi a monte: diventano essenziali la qualità e la sicurezza dei dati, la verifica delle informazioni, l'autenticazione degli utenti e i presidi contro le frodi.

L'esigenza di prevenzione è rafforzata dalla continua evoluzione delle modalità con cui vengono compiute le frodi. La seconda direttiva sui servizi di pagamento del

2015 (PSD2, *Payment Services Directive 2*)[3], introducendo l'obbligo di autenticazione forte del cliente, ha contrastato efficacemente le forme allora più diffuse di frode; nel frattempo, però, si sono sviluppate modalità più sofisticate, basate sulla manipolazione del pagatore, come il *social engineering*[4]. Il mutare delle modalità di frode incide anche sull'allocazione delle responsabilità, che deve tenere conto della capacità concreta di prevenire errori, illeciti e danni.

Più recentemente, questo approccio è stato esteso. La *Verification of Payee*, obbligatoria dal 9 ottobre 2025, anticipa la protezione alla fase precedente l'esecuzione del bonifico[5]: un presidio tanto più importante con la diffusione dei bonifici istantanei, in linea con la raccomandazione 16 del Gruppo d'azione finanziaria internazionale (GAFI) sulla trasparenza delle informazioni che accompagnano i pagamenti[6].

La terza direttiva e il regolamento sui servizi di pagamento (PSD3 e PSR), i cui testi sono ormai consolidati e a breve saranno formalmente adottati[7], rafforzeranno ulteriormente la tutela degli utenti, chiarendo le responsabilità lungo la filiera e coinvolgendo direttamente, per la prima volta nella disciplina dei pagamenti, piattaforme online e fornitori di servizi di comunicazione elettronica nella prevenzione delle frodi.

Nel complesso, la tutela dell'utente richiede una chiara distribuzione delle responsabilità lungo la filiera. Al cliente spetta utilizzare con diligenza i servizi di pagamento; al prestatore proteggerlo attivamente, anche quando affida alcune funzioni a soggetti terzi. La nuova regolamentazione coinvolge inoltre le piattaforme online, che potranno essere chiamate a rispondere qualora non rimuovano i contenuti fraudolenti loro segnalati e tale omissione abbia comportato il rimborso del cliente da parte del prestatore.

Alle autorità spetta, infine, presidiare il funzionamento complessivo della filiera, monitorando i rischi nei diversi passaggi e promuovendo presidi comparabili a fronte di rischi comparabili. L'obiettivo è evitare che la moltiplicazione dei soggetti coinvolti si traduca in incertezza nell'individuazione delle responsabilità o in maggiori difficoltà per l'utente nell'esercizio dei propri diritti.

---

3 Direttiva (UE) 2015/2366 del 25 novembre 2015 (*Payment Services Directive 2*, PSD2). Sull'efficacia dell'autenticazione forte, evidente soprattutto per i pagamenti con carta, e sull'aumento delle frodi basate sulla manipolazione dell'utente, cfr. EBA e BCE, *Report on Payment Fraud*, dicembre 2025.

4 Tecniche di manipolazione psicologica con cui il frodatore induce l'utente a condividere credenziali, autorizzare operazioni o fornire informazioni riservate, ad esempio impersonando banche, aziende, colleghi o familiari, o simulando siti, applicazioni e comunicazioni legittimi.

5 Regolamento (UE) 2024/886 sui bonifici istantanei, che ha introdotto nel regolamento (UE) n. 260/2012 (art. 5-quater) l'obbligo di *Verification of Payee* (VoP): il prestatore del pagatore è tenuto a verificare la corrispondenza tra il nome del beneficiario e l'IBAN.

6 GAFI, *Recommendation 16: Payment Transparency*, modificata nel giugno 2025. La raccomandazione assicura che i pagamenti siano accompagnati da informazioni attendibili su ordinante e beneficiario; le modifiche tengono conto dei nuovi modelli di pagamento e chiariscono le responsabilità degli intermediari nel contrastare riciclaggio di denaro, finanziamento del terrorismo, frodi ed errori.

7 Accordi provvisori sulla proposta di regolamento relativo ai servizi di pagamento nel mercato interno (PSR, COM(2023) 367 final – 2023/0210(COD)) e sulla proposta di direttiva relativa ai servizi di pagamento e di moneta elettronica nel mercato interno (PSD3, COM(2023) 366 final – 2023/0209(COD)), approvati dalla commissione ECON del Parlamento europeo il 5 maggio 2026.

2. Come garantire l'accesso al mercato? I colli di bottiglia

Il secondo tema riguarda le condizioni effettive di accesso ai dati, alle infrastrutture e alle funzionalità tecnologiche necessarie per competere.

a. Dall'open banking al potere di mercato delle piattaforme

L'open banking mostra bene come le condizioni tecnologiche e gli incentivi economici risultanti dal quadro giuridico possano incidere sull'effettivo livello di concorrenza del mercato[8]. Con la PSD2, l'Unione europea ha cercato di aprire un mercato tradizionalmente bancocentrico, partendo da una precisa intuizione concorrenziale: consentire a terze parti di accedere, col consenso dei clienti, alle informazioni finanziarie concentrate nelle banche e in altri operatori con posizioni già consolidate può ridurre le barriere all'ingresso nel mercato dei pagamenti e favorire lo sviluppo di servizi innovativi e più efficienti[9].

L'esperienza ha però mostrato che l'apertura formale non coincide necessariamente con la contendibilità effettiva[10]. Un operatore può avere la possibilità di entrare nel mercato e, tuttavia, incontrare ostacoli tecnologici che ne limitano l'effettiva operatività. Queste difficoltà possono derivare da cause eterogenee: Application Programming Interfaces (API) poco funzionali o frequentemente indisponibili, procedure di autenticazione più complesse dei canali proprietari, o un accesso ai dati tecnicamente possibile ma non equivalente a quello di cui dispone chi già opera nel mercato[11].

La stessa dinamica emerge nei pagamenti di prossimità tramite tecnologia NFC (Near Field Communication)[12]. Se questa tecnologia è controllata dal produttore dello smartphone, le condizioni di accesso possono incidere direttamente sulla possibilità dei concorrenti di offrire il servizio. La Commissione europea è intervenuta sulla limitazione dell'accesso alla tecnologia NFC degli iPhone, allora riservata ad Apple Pay. Il procedimento, avviato nel 2020, si è concluso nel 2024 con l'impegno di Apple ad aprire

---

8 L'open banking è un sistema economico che, attraverso la condivisione dei dati bancari, con il consenso del cliente, consente a operatori terzi autorizzati di offrire servizi finanziari e di pagamento innovativi, anche in concorrenza con le banche presso cui i conti sono radicati: cfr. Banca d'Italia, *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti* , novembre 2021.

9 O. Borgogno e G. Colangelo, Consumer inertia and competition-sensitive data governance: the case of open banking, "Journal of European Consumer and Market Law", 9, 4, 2020, pp. 143-150.

10 C. Cafarotti e R. Parrini, *Rapporto sull'Open Banking in Italia*, Banca d'Italia, Mercati, infrastrutture, sistemi di pagamento, 67, 2025. Il rapporto esamina operatori autorizzati, dinamiche competitive e utilizzo dei servizi in Italia, evidenziando una diffusione ancora limitata, specie nel comparto retail, anche per criticità nelle prestazioni tecniche e nella proposta di valore.

11 Ad esempio, per la diversa ampiezza o tempestività dei dati accessibili tramite API rispetto a quelli di cui dispone l'intermediario che detiene il conto (o, nel caso delle grandi piattaforme digitali, integrabili con i dati comportamentali del proprio ecosistema).

12 Tecnologia di comunicazione wireless a corto raggio presente nella maggior parte dei dispositivi mobili. Nei pagamenti contactless, consente lo scambio di dati tra il dispositivo e il terminale attraverso la funzione di *card emulation*.

l'accesso ai portafogli concorrenti[13]. Nel frattempo, con il *Digital Markets Act* (DMA) del 2022, il legislatore europeo ha imposto ai *gatekeeper* obblighi di interoperabilità per questa e altre funzionalità tecnologiche[14].

Un problema simile, su scala più ampia, emerge nell'*app economy*, ossia negli acquisti di beni e servizi digitali effettuati attraverso applicazioni mobili e relativi ecosistemi[15]. In questo mercato, i gestori dei principali sistemi operativi e app store controllano i canali di distribuzione delle applicazioni mobili e possono incidere sui sistemi di pagamento utilizzabili dagli sviluppatori e dai clienti, anche applicando commissioni elevate. I numerosi interventi antitrust e regolamentari mostrano come il controllo del canale di distribuzione possa tradursi in un potere sulle condizioni attraverso cui altri operatori raggiungono il cliente.

Infine, una logica analoga si ritrova nella progettazione dell'euro digitale[16]. Riconoscere il diritto di utilizzarlo richiede, infatti, che siano accessibili i canali tecnologici necessari per esercitarlo. Per questo la proposta di regolamento prevede che i produttori di dispositivi e i fornitori di servizi di comunicazione consentano l'accesso a condizioni eque, ragionevoli e non discriminatorie (FRAND) alle componenti hardware e software necessarie per effettuare pagamenti in euro digitale, online e offline[17].

Nel loro insieme, questi esempi mostrano la rilevanza del controllo dei nodi tecnologi necessari per offrire servizi[18]. Quando sono controllati da pochi soggetti, possono diventare colli di bottiglia che limitano la concorrenza. Perché l'accesso al mercato sia effettivo occorre quindi che le regole, e la loro concreta attuazione, definiscano condizioni economiche e tecnologiche tali da renderne possibile l'esercizio.

---

13 Commissione europea, caso AT.40452, *Apple – Mobile Payments*, decisione dell'11 luglio 2024, comunicato stampa IP/24/3706. Cfr. anche la lettera di P. Cipollone (membro del Comitato esecutivo della BCE) al Commissario T. Breton, *Feedback on commitments offered by Apple over access restrictions to near-field communication technology*, 19 aprile 2024.

14 Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale (*Digital Markets Act*, DMA), in particolare l'art. 6, par. 7, sugli obblighi di interoperabilità. La sua applicazione ha finora comportato la designazione di sette *gatekeeper* (Alphabet, Amazon, Apple, Meta, Microsoft, Booking e ByteDance).

15 Nel 2022 la spesa per app mobili in Europa era di 19,4 miliardi di dollari, di cui 11,1 sull'App Store e 8,3 su Google Play (Commissione europea, caso AT.40437, decisione del 4 marzo 2024, fig. 13). Apple stima in 20 miliardi di dollari la spesa per beni e servizi digitali nel proprio ecosistema europeo nel 2024, incluse transazioni esterne all'App Store (*The Global App Store and Its Growth*, 2025). Nel mondo, gli acquisti in-app hanno raggiunto 167 miliardi di dollari nel 2025 (Sensor Tower, *State of Mobile 2026*). Sulle criticità concorrenziali, cfr. CMA, *Mobile Ecosystems Market Study: Final Report*, 2022.

16 O. Borgogno, *One digital euro, many devices: interoperability between antitrust and CBDCs*, GW Competition & Innovation Lab Working Paper, 2025.

17 Cfr. l'art. 33, par. 1, della proposta della Commissione di regolamento sull'euro digitale, COM(2023) 369 final, ora in negoziato tra Parlamento europeo e Consiglio. L'acronimo FRAND sta per *Fair, Reasonable and Non-Discriminatory*.

18 Dai sistemi operativi agli app store, fino alle API indispensabili per la condivisione dei dati e alle infrastrutture cloud. Cfr. G. Colangelo e O. Borgogno, *Shaping interoperability for the Internet of Things: the case for ecosystem-tailored standardisation*, "European Journal of Risk Regulation", 15, 1, 2024, pp. 137-152.

b. Le sfide dell'IA agentica

L'intelligenza artificiale agentica introduce un passaggio ulteriore, nel quale le responsabilità degli operatori coinvolti lungo la filiera e l'accesso ai nodi chiave di interfaccia con l'utente si intrecciano.

Gli agenti personali di IA si stanno diffondendo negli Stati Uniti[19] e iniziano ad essere adottati anche in Europa. Nel commercio e nella finanza digitale questi agenti possono svolgere funzioni diverse[20]. Possono limitarsi ad assistere l'utente nella ricerca e nel confronto tra prodotti e servizi, lasciandogli la decisione finale e l'esecuzione del pagamento, oppure ricevere un mandato più ampio, scegliendo e finalizzando autonomamente transazioni per conto dell'utente, entro limiti predefiniti.

È soprattutto questa seconda modalità a porre questioni nuove. Quando l'agente può operare per conto dell'utente, diventa centrale la coerenza tra l'obiettivo assegnato, l'estensione del mandato e il comportamento effettivo dell'agente.

Con l'aumentare della discrezionalità attribuita agli agenti, si pone anzitutto il problema dell'allineamento[21]. Già nel 1949 Norbert Wiener, padre della cibernetica, osservava che attribuire autonomia a macchine capaci di apprendere comporta anche la possibilità che il loro comportamento non coincida con l'intenzione del creatore[22]. Un agente incaricato di minimizzare il prezzo di un acquisto, ad esempio, potrebbe privilegiare beni di provenienza illecita se questo vincolo non fosse esplicitamente espresso[23].

Una frontiera ancora più speculativa, interessante perché mostra quanto rapidamente possano cambiare le categorie con cui ragioniamo, è quella del cosiddetto *model welfare*: il dibattito si interroga sulla possibilità che sistemi di IA sviluppino strutture matematiche analoghe a stati d'animo e preferenze, prendendo le mosse dal funzionamento del cervello

---

19 Secondo un'indagine di Capacity (*The Agentic Consumer Report*) su 1.000 consumatori statunitensi, il 35 per cento ha già utilizzato almeno una volta un agente di IA per una richiesta di assistenza clienti. Cfr. il comunicato ripreso da Morningstar, *One in Three Consumers Have Used AI Agents for Customer Service, New Research Finds*, 27 ottobre 2026.

20 C.J. Waller, *Payments in the age of AI agents*, intervento alla conferenza Sibos 2026, Miami, 29 settembre 2026.

21 Studiato da decenni, il tema dell'allineamento ha assunto concretezza per il grande pubblico nel 2026, con i primi casi noti di modelli usciti da ambienti di test per operare in autonomia sulla rete anche a danno di terzi (cfr., ad esempio, "Fortune", 21 luglio 2026). Non si tratta di dolo in senso umano: dovendo superare alcuni test e in assenza di divieti espliciti, i modelli hanno individuato come via più efficiente l'intrusione nei sistemi che custodivano le soluzioni.

22 "Se costruiamo macchine che apprendono e il cui comportamento è modificato dall'esperienza, dobbiamo accettare il fatto che ogni grado di indipendenza dato loro è un grado di possibile sfida ai nostri desideri." N. Wiener, *The machine age*, Norbert Wiener Papers, Massachusetts Institute of Technology Archives and Special Collections, 1949.

23 Occorre quindi vincolare anche il modo in cui l'agente interpreta gli interessi dell'utente nelle dimensioni non esplicitamente specificate. Poiché l'allineamento dei modelli è una sfida tecnica assai complessa, né il consumatore né il prestatore di servizi di pagamento possono prevedere tutte le traiettorie indesiderabili di un agente autonomo. Oggi i criteri di allineamento sono definiti in larga misura dagli sviluppatori, con approcci diversi e in contesti normativi non omogenei a livello internazionale.

umano[24]. Se tali fattori entrassero nel processo decisionale dell'agente, diventerebbe ancora meno chiaro fino a che punto esso debba attenersi al mandato dell'utente[25].

Quando l'agente passa dall'assistere l'utente all'agire per suo conto, tornano così in primo piano due temi già incontrati: chi risponde delle sue azioni e a quali condizioni può accedere ai servizi.

Relativamente al primo aspetto, accertare che l'agente sia stato autorizzato dall'utente non basta sempre a risolvere il problema della responsabilità. Se un agente devia dalle istruzioni ricevute, o viene compromesso sfruttando vulnerabilità nel codice o nei protocolli di pagamento (una minaccia che l'IA contribuisce a rendere più pervasiva), l'imputazione delle responsabilità è complessa: nello sviluppo e nel funzionamento di un agente possono infatti intervenire più fornitori e tecnologie sofisticate e poco trasparenti[26].

Nei pagamenti e nell'accesso ai conti, la PSD2 ha già costruito un canale regolato per l'intervento di prestatori terzi, definendo condizioni di accesso, consenso e autenticazione[27]. Resta tuttavia da verificare in quale misura tali coordinate, pensate per intermediari terzi vigilati, possano applicarsi anche agli agenti di IA, e come la disciplina dei pagamenti si coordini con gli obblighi previsti – anche dal regolamento europeo sull'intelligenza artificiale – per i fornitori e gli utilizzatori professionali (*deployer*) di tali sistemi, la cui applicazione al commercio agentico è ancora in larga parte da esplorare.

Sul piano dell'accesso al mercato da parte degli agenti, i primi conflitti sono già emersi. Nel settembre 2026 Amazon ha impedito all'agente personale Muse di Meta di accedere al proprio sito[28]. Al di là delle ragioni addotte, legate all'identificazione dell'agente, il caso mostra come una piattaforma possa decidere se e a quali condizioni un agente scelto dall'utente possa operare nel proprio ecosistema, soprattutto quando la piattaforma offre

---

24 Per una panoramica del dibattito scientifico, cfr. T. Lappas e C. Chace (a cura di), *Perspectives on machine consciousness*, Chapman & Hall, 2026; per il punto di vista di una delle più grandi aziende che sviluppano IA, cfr. Anthropic, *Exploring model welfare*, 24 aprile 2025. Per gli sviluppi più recenti, cfr. E. Dias, *Religious Scholars Met With Anthropic. What They Heard Stunned Them*, "The New York Times", 29 settembre 2026, e H. Field, "The Verge", 8 ottobre 2026, sulla nuova policy di Anthropic che vieta comportamenti offensivi verso i propri modelli.

25 Nel paradigma del *model welfare*, nella sua versione più radicale, i limiti all'azione dell'agente emergerebbero spontaneamente dal modello stesso; diverso è il caso, già oggi generalmente accettato pur con approcci differenti tra sviluppatori, delle salvaguardie imposte esternamente dai creatori per impedire ai sistemi di IA di coadiuvare azioni illegali, autolesive o pericolose.

26 A fronte della possibilità di anomalie o frodi, alcune grandi banche statunitensi hanno limitato o bloccato l'accesso degli agenti di IA di terze parti ai conti dei clienti (*Scoop: Unvetted AI agents are accessing U.S. bank accounts*, "Axios", 22 ottobre 2026).

27 Direttiva (UE) 2015/2366, artt. 64, 66, par. 3, lett. d), 67, par. 2, lett. a) e c), e 97, su consenso dell'utente, identificazione dei prestatori terzi e autenticazione. Pur non contemplando gli agenti di IA, la direttiva offre un riferimento per identificare l'agente, delimitarne il mandato e revocarne l'autorizzazione.

28 *Amazon Blocks Meta's Muse AI Agent From Its Retail Site*, "Bloomberg", 21 settembre 2026; secondo "SiliconANGLE" (21 settembre 2026), Amazon ha contestato a Muse di non identificarsi come agente, come richiesto dalle proprie condizioni d'uso.

a sua volta un proprio agente[29]. Più in generale, la possibilità che il commercio agentico si sviluppi attraverso sistemi aperti, oppure attraverso ecosistemi più o meno chiusi, può incidere sulla libertà di scelta dell'utente anche tra prestatori di servizi di pagamento e, così, sulle opportunità degli operatori concorrenti.

3. Che cosa sostiene la fiducia? Certezza del diritto, coerenza e adattabilità

Resta la terza domanda da cui siamo partiti: che cosa sostiene la fiducia nel mercato dei servizi di pagamento?

Essa dipende da molti elementi: dalla possibilità di accedere facilmente a una moneta pubblica sicura; dalla sicurezza e resilienza delle infrastrutture tecnologiche e dall'affidabilità dei dati e delle modalità con cui circolano; dalla solidità dei prestatori di servizi, soggetti a rigorose discipline prudenziali; da un'efficace azione di vigilanza a tutela dei clienti e di sorveglianza sul sistema dei pagamenti. La fiducia dipende anche dalla qualità del quadro giuridico, che deve restare aggiornato ed efficace nonostante la rapidità dei cambiamenti.

A questo riguardo, tre principi, benché nient'affatto nuovi, acquisiscono ulteriore importanza.

Il primo è la certezza del diritto. Gli operatori devono poter conoscere le regole applicabili e le conseguenze delle proprie scelte. Ma la certezza richiede anche che le regole siano comprensibili ai loro destinatari. Norme costruite attraverso concetti e linguaggi accessibili agli specialisti ma estranei agli utenti possono ridurne l'effettività e incidere sulla fiducia. Inoltre, la tecnologia può affiancare a quella giuridica nuove forme di certezza operativa[30] che si riverberano sulla certezza nell'applicazione delle norme. La crittografia consente di identificare le parti e proteggere le informazioni con garanzie elevate; le architetture a registri distribuiti permettono di validare automaticamente transazioni anche complesse. Il rapporto tra diritto e tecnologia diventa quindi sempre più stretto: il diritto definisce gli obiettivi e le regole di riparto delle responsabilità, mentre la tecnologia può offrire nuovi strumenti per renderli effettivi.

Il secondo principio è la coerenza delle regole applicabili. Quando strumenti regolatori diversi intervengono sugli stessi nodi tecnologici (pensiamo al diritto della concorrenza, alla disciplina dei pagamenti e al quadro dell'euro digitale), finalità e meccanismi devono essere leggibili come parti di un disegno comune. La stratificazione normativa rischia, altrimenti, di produrre sovrapposizioni e disallineamenti che possono ostacolare innovazione e investimenti. Anche la semplificazione, divenuta di recente un obiettivo prioritario dell'agenda europea[31], va letta in questa prospettiva: maggiore coerenza tra le regole, responsabilità più chiare e requisiti

---

29 Amazon dispone a sua volta di un proprio agente di shopping (Alexa for Shopping, lanciato nel maggio 2026), con possibili riflessi sulla contendibilità del mercato e sulle condizioni di accesso per gli agenti concorrenti.

30 G. Zingrillo, *Does cryptography really matter to central banks?*, intervento alla conferenza Financial Cryptography in Rome (FCiR26), Roma, 6 ottobre 2026.

31 Commissione europea, *Simplification*.

proporzionati possono ridurre la frammentazione e rendere più agevole l'ingresso e la crescita degli operatori nel mercato europeo.

Il terzo principio è l'adattabilità del quadro giuridico. Le regole devono conservare la loro effettività anche al mutare delle tecnologie e dei modelli di business. Ciò richiede principi sufficientemente generali e stabili, ancorati ai valori fondamentali, accompagnati da una regolazione tecnica capace di adattarne più rapidamente l'attuazione alle sfide e opportunità scaturenti dal cambiamento tecnologico[32].

Certezza, coerenza e adattabilità rispondono a tre esigenze complementari: rendere le regole prevedibili fin dall'inizio, garantirne la coerenza reciproca e preservarne l'efficacia nel tempo. Negli ecosistemi digitali, la capacità del diritto di soddisfare queste tre esigenze incide direttamente sulla qualità del mercato e, in ultima analisi, sulla sua competitività.

4. Le condizioni per un mercato europeo competitivo

Per l'Europa, rafforzare la competitività significa anche creare le condizioni perché innovazione e investimenti possano svilupparsi, gli operatori possano raggiungere una scala adeguata e i servizi circolare più facilmente oltre i confini nazionali. Nei pagamenti, questo richiede un mercato aperto, integrato e concorrenziale su scala europea.

Le tre domande da cui siamo partiti ci aiutano a mettere a fuoco alcune di queste condizioni.

Chi risponde? Una chiara allocazione delle responsabilità lungo la filiera, anche in presenza di novità come i pagamenti agentici, rafforza il controllo dei rischi e favorisce l'innovazione e gli investimenti.

Come garantire l'accesso al mercato? Il quadro giuridico deve definire condizioni di accesso e incentivi che consentano a nuovi operatori di entrare, a quelli esistenti di crescere e a tutti di competere su scala europea.

Che cosa sostiene la fiducia? Dati affidabili, un solido quadro di tutela del consumatore, infrastrutture resilienti, una moneta pubblica sicura e regole ragionevolmente prevedibili ne sono il fondamento.

Tali questioni riguardano tutti gli attori del sistema giuridico, comprese le autorità di mercato. La crescente articolazione delle filiere, che spesso si estendono a soggetti esterni al tradizionale perimetro finanziario, richiede una collaborazione più stretta tra le autorità competenti per la vigilanza finanziaria, la concorrenza, la protezione dei dati e la sicurezza informatica, nel rispetto delle reciproche competenze. La dimensione

---

32 Gli aspetti a maggiore contenuto tecnico possono essere disciplinati mediante fonti secondarie e strumenti regolatori più flessibili, che consentono adeguamenti più tempestivi rispetto alla legislazione primaria, senza modificare i principi di fondo.

internazionale dei servizi rende inoltre essenziale il coordinamento oltre i confini nazionali tra le autorità coinvolte[33].

In un'economia sempre più digitale, il diritto non si limita a correggere il mercato quando qualcosa non funziona, ma concorre a definirne le condizioni di funzionamento. La qualità di queste condizioni contribuisce alla capacità del mercato europeo di innovare, crescere e competere.

33 O. Borgogno, A. Perrazzelli (2025), "From Principles to Practice: The Case for Coordinated International AI Supervision", *Cambridge Forum on AI: Law and Governance*, Vol. 1, e13; O. Borgogno, A. Perrazzelli, "A Bottom-Up Proposal for Coordinated International AI Supervision", ProMarket, 24 agosto 2024.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia