

CONTRARIAN

FINTECH ALLA PROVA DEL DIRITTO CIVILE URGE RISPOSTA EUROPEA

► In una realtà sempre più digitalizzata, il settore finanziario sarà sempre più impattato dal fintech ossia dal prodotto dell'incontro tra nuove tecnologie e finanza. Già da qualche anno infatti la rivoluzione digitale ha generato prodotti finanziari, modelli di business e forme di negoziazione nuovi, che affiancano e talora soppiantano le tradizionali modalità di investimento, consulenza e ricerca di capitali. Provvisoriamente sospesa dall'emergenza Covid, quest'autunno dovrebbe partire la Conferenza sul futuro dell'Europa promossa dal parlamento Ue e dovrebbe prendere nuovo slancio la strategia digitale europea della Commissione, che sta altresì lavorando su nuove norme sui servizi digitali. L'intelligenza artificiale e il machine learning, la disponibilità di big data e servizi cloud, le distributed ledger technology, le numerose piattaforme finanziarie on-line hanno ridisegnato profondamente il settore finanziario consentendo l'emergere di nuovi asset, come le cryptovalute, forme d'investimento su nuove piattaforme, sistemi di consulenza robotica, smart contract. L'urto dell'universo algoritmico ha dunque prodotto preoccupazioni regolamentari, anche per la natura cross-border dei fenomeni (che li sgancia da legislazioni e procedimenti nazionali). Chi può operare, a quali condizioni, sotto quale forma di vigilanza è dunque il primo (irrisolto) cruccio. L'avvento del General data protection regulation e la protezione dei dati personali ha poi fatto emergere ulteriori problemi, acuiti dalle limitazioni al trasferimento di dati extra-Ue come effetto della sentenza Schrems II della Corte di giustizia. Ma il fintech pone problemi anche rispetto al regime delle responsabilità e alla law of contract. Che cosa succede se viene prodotto un danno come effetto dell'uso di un sistema d'intelligenza artificiale applicato a un robo-advice o a una piattaforma peer-to-peer? Rispondono l'utilizzatore, il programmatore, il manutentore o il gestore? E che tipo di responsabilità può essere predicata (per mancata vigilanza) rispetto all'autorità preposta ai controlli? Infine, che tipo di responsabilità 231 può nascere, anche sotto un profilo di cybersecurity, nel caso di malfunzionamento di un sistema robotico applicato al Kyc o alla compliance? Dubbi di natura contrattuale sorgono anche intorno alla blockchain. La tecnologia distribuita consente di registrare transazioni commerciali (di bitcoin, ma non solo) su vari nodi informatici in modo condiviso, immutabile e permanente. In tal modo, la cessione di bitcoin da A a B e l'ingresso di tali monete virtuali nell'e-wallet di B viene registrato su tutti i nodi e non può essere alterato se non con il consenso di tutti i partecipanti. Tutto ok, ma solo finché l'operazione non sia colpita da una delle forme d'invalidità, risoluzione o inefficacia previste dal diritto dei contratti (nullità, annullamento, simulazione, revoca, risoluzione, rescissione). Se questo accedesse, infatti, la cessione registrata nella blockchain potrà certamente essere smontata con un ritrasferimento dal compratore al venditore, ma ciò avrà effetto solo dal momento in cui sarà stata compiuta (ex nunc) e non già, come invece imporrebbe il diritto civile, con effetto retroattivo (ex tunc) da quando l'operazione primigenia invalidata è stata compiuta. Nel caso poi di smart contract negoziati ed eseguiti attraverso protocolli informatici, che spazio potranno avere i concetti di dolo ed errore, approfittamento o buona fede? È urgente allargare lo sguardo, non limitandosi

agli aspetti autorizzativi e regolamentari della digital economy, ma trovando meccanismi percorribili anche dal punto di vista del diritto civile che inevitabilmente guiderà giudici ed arbitri nella soluzione dei casi controversi. La strategia europea della regolazione dovrà farsi carico anche di questo. (riproduzione riservata)

*A cura di Andrea Fedi
Partner, Legance - Avvocati Associati*

