Dati e finanza: nuove opportunità e nuove vulnerabilità.
La necessità di cambiare paradigma

Paolo Ciocca
Commissario Consob
Roma, 18 novembre 2020

Buongiorno.
Ringrazio il Presidente Patuelli, il Direttore Generale Sabatini e voi tutti per l'opportunità di essere oggi qui con voi.
È per me un vero piacere personale tornare a parlare in Associazione, dove ho avuto l'opportunità di lavorare ormai diciotto anni fa, su questioni diverse da quelle di cui discuteremo oggi. Ma la prospettiva che viene con l'età e con le diverse esperienze professionali mi lascia pensare che forse questa distanza è solo apparente.

CMU, rivoluzione tecnologica, competizione europea e globale

La Commissione ha recentemente presentato la sua *roadmap* per la CMU. Si tratta di un progetto importante che punta a un risultato ambizioso; direi essenziale perché il mercato europeo sia all'altezza della sfida globale post-Covid e post-Brexit. Abbiamo bisogno di una piazza finanziaria regionale più profonda e meno frammentata per soddisfare la sete di *equity* delle nostre imprese che vogliono crescere e cogliere le opportunità offerte dall'innovazione tecnologica. Non è quindi un caso che il programma della Commissione presenti quale primo obiettivo a breve termine l'ESAP, cioè la realizzazione di una "infrastruttura" informativa che funga da punto di accesso unico al compendio informativo, finanziario e non, degli emittenti, incluso quello sulla sostenibilità; ciò per favorire la comparazione dei dati, la visibilità anche transfrontaliera delle nostre imprese e l'efficienza allocativa dei mercati UE. Il progetto è completato dalle recenti iniziative legislative in materia di finanza digitale, che forniscono sostanza alla CMU. Si pongono quindi i presupposti regolatori affinché l'Unione possa compiutamente rispondere alla sfida competitiva che su questo campo proviene sia da occidente che da oriente.

Ma nel frattempo il mercato si muove: si pensi alle recenti operazioni Euronext/Borsa Italiana e LSEG/Refinitiv. In sintesi, assistiamo, da un lato a un consolidamento regionale (orizzontale) di importanti società di gestione del mercato, che quindi la CMU la realizzano concretamente. Dall'altro, a un consolidamento (verticale) di segmenti di attività accomunati dall'utilizzo e dalla valorizzazione di big data finanziari. In questo secondo caso è evidente l'ambizione di creare un *player* globale che sfrutti appieno l'integrazione tra fonti di dati diverse.

Si tratta a tutta evidenza di una competizione globale, su di un terreno - quello dei dati e delle infrastrutture su cui transitano - altamente sensibile: quando si tratta di dati, la sicurezza nazionale (e regionale) è un elemento necessario ed ineludibile. Come vedremo più avanti, l'incrocio tra sicurezza nazionale e sicurezza comunitaria non si declina facilmente, per cui sono necessari approcci nuovi.

Tecnologie* digital enabler*: ma quali?

Di quali tecnologie innovative stiamo parlando? Molte delle applicazioni sono ben conosciute: *roboadvice*, *algotrade*, profilazione dei clienti solo per citarne alcune di quelle presenti nel *front office*

degli intermediari; oppure analisi automatizzata, *AML* ed antifrode, per quelle nel *back office*. Queste, come le altre sono generalmente riconducibili ad alcune tecnologie fondanti: *Cloud Computing, DLTs, Big Data & Machine Learning*, intelligenza artificiale.

Il Cloud Computing non è certo una nuova tecnologia tanto essa ormai pervade ampiamente il mercato dell'informatica globale. Il Covid, con il ricorso globale al lavoro a distanza, ha messo in luce il carattere infrastrutturale di questo servizio, che rappresenta il presupposto, il *playing field*, nel quale muovono le altre innovazioni. Trainato dall'efficientamento economico ed architetturale delle infrastrutture informatiche aziendali, il *Cloud Computing* muta profondamente la mappa delle opportunità e dei rischi degli intermediari e delle autorità di vigilanza, e determina l'*outsourcing* con accentramento sia dei dati che delle elaborazioni, anche le più sensibili. Sul lato dell'offerta, il mercato non conosce un solo grande *provider* europeo che possa competere alla scala di quelli globali. Di qui l'importanza della recente iniziativa europea *Gaia-X*, che cerca di sovvenire con una *partnership* pubblico/privato a questa assenza. L'iniziativa si basa su di un forte coordinamento regolatorio, piuttosto che su una artificiale (ed improbabile) ipotesi di creare dal nulla un *Bigtech* UE. A questo proposito, la recente proposta di regolamento DORA rappresenta la giusta risposta con un quadro unitario UE per la vigilanza dei maggiori *provider* (concorrenza del regolatore europeo e di quelli nazionali), nonché la fissazione di obiettivi di risultato - piuttosto che di sola *compliance* - sia per gli intermediari finanziari che per le autorità. Questo non basterà: perché la regione europea possa competere effettivamente nel confronto globale, sarà necessaria una partecipazione convinta alle iniziative europee, quali appunto Gaia-X, sia del mercato che delle autorità pubbliche europee e nazionali.

Le *DLT* si stanno progressivamente facendo strada soprattutto nel *backoffice*, con la loro innata capacità di fornire certezza delle transazioni mediante un sistema di controllo decentrato e condiviso. Consob, con i suoi approfondimenti dapprima in materia di *ICOs* ed ora di *STOs*, ha acquisito un ragguardevole *know-how* regolatorio. In questo senso, si avvicina il momento di condividere una riflessione sulle più opportune modalità di regolare l'emissione - con tecnologia *DLT* - di vere e proprie *security*, anche alla luce della crescente domanda da parte di attori di mercato. I vantaggi, in termini di riduzione dei costi di emissione, sono importanti. L'attenzione del regolatore si deve concentrare sulle garanzie sostanziali che occorre fornire ai sottoscrittori, sia in termini di circolazione che di liquidità dei titoli. Le recenti proposte di regolamenti comunitari MICA e PILOT, nel confermare pienamente l'analisi preliminare di Consob, rappresentano un importante passo in avanti per la sistemazione compiuta di un mercato finanziario digitale: MICA permette di definire *criptoasset* che non rappresentano *securities*; PILOT apre la strada alla sperimentazione di un mercato secondario per questi strumenti. I nuovi strumenti potranno circolare liberamente nel mercato UE ed il nostro è certamente un mercato di sbocco: alla luce di ciò, nelle negoziazioni che si stanno conducendo, sarà necessario porre la massima attenzione affinché, fermo restando il supporto all'innovazione, non si assista a uno svuotamento delle tutele previste da MiFID. I profili definitori e il livello di armonizzazione delle condizioni di accesso al mercato interno saranno i temi cruciali.

Big data e advanced analytics: la vera rivoluzione sta nella disponibilità di una vastissima mole di dati, finanziari e non, su cui condurre analisi ed elaborazioni mediante algoritmi predittivi. Si tratta del noto circuito: dati, informazione, conoscenza, sapienza. Rilevano le tecnologie di elaborazione basate sul *machine learning*, che permettono di trattare (*i.e.*, raccogliere, comporre, estrarre, ordinare, incrociare, correlare, etc.) queste immense quantità di dati. Siamo ancora nel campo di - sia pur elaborate - tecniche; esse registrano importanti accelerazioni sia nel campo finanziario che in quello non finanziario. Ad esempio, se per ora la robotica non sembra rappresentare un elemento cruciale per

il settore finanziario, altrettanto non si può certo dire per le tecniche di riconoscimento facciale: queste ultime, nate per rispondere ad esigenze di ordine pubblico, stanno trovando piena applicazione in campo finanziario ad esempio in Cina. In materia di *machine learning* i punti più avanzati di ricerca toccano questioni assai rilevanti, anche per il sistema finanziario, quali la capacità di estrarre correlazioni tra basi dati senza necessità di conoscere il contenuto in chiaro delle stesse, ovvero la capacità di valutare ex ante la potenzialità di avanzamento degli stessi algoritmi.

Più in generale, nel campo dell'intelligenza artificiale vera e propria, i progressi avanzano assai veloci, mentre si riducono i tempi per la definizione di tecnologie affidabili per la diretta connessione macchina-uomo; e qui la storia è ancora tutta da scrivere.

Questa è l'area che pone per intermediari e regolatori le sfide più importanti.

Alcune fra le tante: come controllare l'attività di algoritmi sofisticatissimi e che autoapprendono (e per i quali non è possibile predire l'evoluzione dell'attività) che - per definizione - non sono analizzabili ex ante?
Il principio del *machine learning* si basa sull'apprendimento di un algoritmo da un set di dati per poi essere applicato in diretta: come evitare il *bias* (di qualsiasi tipo) che può derivare dai limiti della base di apprendimento?
Si pensi ai rischi reputazionali per un intermediario di un *bias* insito nell'algoritmo e non compreso fino a quando non si verifichino gli effetti, ad esempio nell'elaborazione dei processi di affidamento, nella profilazione dei clienti. Inoltre, non trattandosi di un software ordinario - per il quale si potrebbe in astratto invocare una responsabilità del fornitore - qui l'algoritmo sviluppa ed affina le sue capacità di analisi e scelta (magari errate) solo all'interno dei sistemi del singolo intermediario, con tutte le conseguenze del caso.

Queste sfide, molte delle quali *cross-industry*, sono attualmente oggetto di studio della scienza dei dati, ed i risultati di questi studi saranno certamente cruciali anche per l'attività dei regolatori e degli intermediari. L'industria finanziaria è all'avanguardia nello sviluppo di queste tecnologie, e gli investimenti del settore finanziario sono certamente tra i più importanti.

Allo stesso tempo - ed a maggior ragione - occorre che ci sia piena consapevolezza da parte del sistema di questi (nuovi) rischi. La consapevolezza deve pervadere la *corporate governance* del singolo intermediario a tutti i suoi livelli: il *tone from the top* è essenziale.

Il rapporto continuo tra industria - singola ed associata - e ricerca è fondamentale e rappresenta la chiave di volta strategica per affrontare la rivoluzione.

Dove si posizionano i* Bigtech*?

Si potrebbe dire: ma questi problemi sono gli stessi che deve affrontare un *Bigtech* non finanziario, che per primo (e meglio) fa uso proprio di queste tecnologie? Qui interviene il differente grado di regolazione dei due settori, *Bigtech* e finanziario, e delle diverse attitudini degli attori di mercato. Da un lato gli intermediari finanziari - *incumbent* ed innovativi nativi - che si affacciano all'applicazione progressiva delle tecnologie, dall'altro i *Bigtech* che si avvicinano al settore finanziario. Mi sembra d'intravedere la scelta opportunistica dei *Bigtech* nello scegliere il campo di gioco a partire da quei segmenti di attività in cui: i) la tecnologia è preponderante, ii) il (percepito) rischio reputazionale è

minore. Di qui il crescente interesse dei *Bigtech* per il sistema dei pagamenti, piuttosto che non per i servizi *core* (*lending* ovvero emissione di *asset* finanziari).

Due brevi digressioni.

La prima di carattere globale. Se questo quadro vale per il sistema finanziario occidentale, ben diversa è la situazione a oriente: si pensi all'ecosistema finanziario cinese che, attraverso le *superapp*,permette ai *Bigtech* locali di offrire un'amplissima gamma di servizi finanziari direttamente ai clienti. Gli effetti di *disruption* anche architetturale sono evidenti nelle recenti tensioni istituzionali emerse in occasione della progettata (e poi ritirata) IPO di Antfinancial. La sperimentazione dei servizi *core* avviene in mercati dove condizioni economiche e regole meno stringenti facilitano tali processi; e questi attori si troveranno quindi presto pronti a fare il salto anche in mercati più avanzati.

La seconda è invece di metodo: la variabile determinante di questa equazione competitiva tra i due settori è certamente il tempo. Se il tempo dato al settore finanziario per prepararsi alla sfida era sin qui ridotto, per effetto del Covid questo tempo è sostanzialmente finito. Gli effetti di isolamento necessitati dalla pandemia hanno beneficiato quei soggetti che basano il proprio modello produttivo sull'effetto rete, *Bigtech* in particolare. Facile previsione è quella per cui lo scenario competitivo post-Covid, in particolare nel settore finanziario, registrerà un vantaggio per gli attori non convenzionali o comunque in grado di sfruttare l'effetto rete.

Torno al punto principale, per concludere.

Questa pressione competitiva "esterna" deve stimolare gli operatori tradizionali a innovare di più e più in fretta, sfruttando l'enorme ricchezza derivante dal proprio patrimonio informativo e dalle opportunità che offre la condivisione dei dati a livello UE, anche mediante investimenti e modelli di collaborazione con il mondo Fintech. Adesso o mai più.

***Un vecchio concetto nel nuovo mondo:* trust**

Ma mondo dei dati e finanza hanno certamente qualcosa in comune. Un elemento fondante per entrambi è la fiducia, *trust*. Questo vale sia a livello di settore che individualmente. Facile il riferimento agli effetti delle crisi di fiducia nel settore finanziario; altrettanto importanti i casi di crisi di fiducia per alcuni *Bigtech* (FB fra tutti). La fiducia è la risultante di un complesso di fattori: stabilità finanziaria, reputazione, sicurezza, fra gli altri.

Mi soffermerò sull'aspetto della sicurezza. *Cybersecurity* non equivale a sicurezza informatica. Si tratta di un concetto assai più ampio, che tiene conto delle mutate condizioni di contesto tecnologico, economico e geopolitico.

Contesto tecnologico: valgono l'accelerazione dell'innovazione, l'ampliamento a dismisura della rete di connessione, le prospettive di connessione completa *IoT*, la correntezza di condivisione dei dati su piattaforme tecnologiche. Secondo un canone di sicurezza basilare, un aumento della superficie di attacco determina un incremento della vulnerabilità. A seconda del contesto, l'incremento può essere ben più che proporzionale. L'attacco *cyber* è tecnicamente tracciabile con estrema difficoltà, e solo in pochi casi in tempo reale. Allo stesso tempo, lo strumento *cyber* ha una flessibilità operativa al limite infinita. Da ultimo, in un sistema basato su connessioni a rete, anche l'ultimo anello della catena può rappresentare una vulnerabilità per tutto il sistema.

Contesto economico: perché a questa accelerazione tecnologica sono associate porzioni di valore aggiunto sempre maggiori, sia a livello macro che micro. Ciò determina un interesse crescente per l'attore ostile, tradizionale (ladro, terrorista, etc.) o statuale.

Ma vi è anche la somma dei due cioè la disponibilità di nuove "armi", di nuovi *malware* complessi a prezzi assai ridotti (nell'ordine delle centinaia di migliaia di euro), con effetti di incremento esponenziale del rischio. Per l'attore ostile quello che conta è il valore di impatto: si pensi a un *malware* che porti al blocco, anche solo parziale, di un'infrastruttura finanziaria principale quale la borsa; il valore effettivo dipende dall'impatto percepito, giacché i mercati sono connessi (es. un sistema di borse regionale); data la centralità degli attori del sistema finanziario rispetto agli altri settori economici ed al pubblico in generale, il valore di impatto ultimo è ancora più grande; infine, in un contesto informativo *social*, il valore di impatto può facilmente essere amplificato attraverso la disinformazione.

Abbiamo ricordato anche la componente geopolitica. La difficoltà (tecnica) di attribuzione degli attacchi comporta l'assenza di chiare regole, riconosciute dalla comunità internazionale, volte a sanzionare il comportamento ostile. Ciò, insieme all'alta remunerativà dell'attacco *cyber*, ha determinato una modifica strutturale dell'equazione strategica di rischio/opportunità e dello stesso concetto di deterrenza. L'analisi strategica ha ormai unanimemente identificato quello che rappresenta a tutti gli effetti uno stato di conflitto non dichiarato, al di sotto del livello internazionalmente riconosciuto dell'atto bellico proprio (che dà diritto a una risposta proporzionata); e questo conflitto si svolge (quasi) esclusivamente nel terreno non militare.

Il settore finanziario, per la sua centralità strategica, è al centro di questo contesto conflittuale.

Queste considerazioni vanno portate a sistema, per cogliere l'effetto complessivo per il sistema finanziario, le sue infrastrutture e per i singoli intermediari.

Il fatto che vi sia una difficoltà tecnica nell'attribuzione degli attacchi *cyber* non vuol dire che gli Stati non abbiano altri strumenti per valutare l'attribuibilità di un attacco e per comprendere attore e motivi (*who&why*). Ma solo lo Stato dispone del quadro complessivo di informazioni/fattori (la famosa matrice *DIMEFIL*) che stanno dietro un attacco cyber. Quindi, il rapporto con lo Stato - con i suoi organi di tutela della sicurezza nazionale e di *law enforcement* - diviene un elemento cruciale, soprattutto nelle situazioni più complesse.

Altrettanto fondamentale è l'attitudine del *management* a tutti i livelli, del CdA, degli organi di controllo. Anche qui vale il *tone from the top.* Si tratta di evolvere da una cultura della *compliance* (*tick the box attitude*) a una della resilienza: non è questione del se, ma del quando e del come. L'intermediario e l'infrastruttura finanziaria devono quindi scegliere la propria postura difensiva rispetto a un *framework* che, fatti salvi i livelli minimi di difesa comunque necessari, definisca il livello di protezione che l'organizzazione si prefigge. Il tutto attraverso un processo di scelta cosciente, validata dai diversi organi aziendali.

Alla luce di quanto precede è forse ora meglio delineabile il carattere fondante della proposta di regolamento UE DORA: un *big bang* della *cyber security* per il sistema finanziario comunitario, con obiettivi comuni sfidanti. Un effetto di istantaneo innalzamento dello *standard* regionale, che rende il sistema finanziario comunitario più forte e con ricadute anche globali: simile quindi - ancorché su un

terreno diverso - all'effetto a suo tempo determinato da GDPR. E con una scelta del tempo assai opportuna, cioè appena a ridosso della Brexit.

Nella negoziazione del regolamento, un tema che certamente richiederà approfondimento è quello che sta all'intersezione tra competenze comunitarie degli organi di vigilanza (nazionali e comunitari) e questioni di sicurezza nazionale, la cui competenza resta al momento esclusivamente in capo agli Stati membri. È un terreno questo ancora tutto da esplorare.

Quali spunti per la riflessione strategica del settore finanziario italiano

«*Il ruolo del mercato è centrale nel processo di ripresa del Paese che ha subito una crisi sanitaria senza precedenti, con gravi effetti economici e sociali, e conseguenze ancora difficili da valutare nella loro complessità*» ha ricordato il Presidente della Repubblica in occasione dell'incontro annuale della Consob con il mercato finanziario, lo scorso giugno.

Dal Covid usciremo diversi, individualmente e nei rispettivi ruoli istituzionali ed aziendali. Per quanto attiene al tema di oggi, ho già detto: il tempo per cogliere l'opportunità della trasformazione è finito.

Il sistema finanziario nazionale deve a mio parere abbracciare in pieno l'accelerazione tecnologica. E fare dei propri punti di forza - quali l'ampiezza del contenuto informativo raccolto nella propria attività, la naturale capacità di interconnessione tra i vari intermediari, la dimensione corrente e futura degli investimenti in tecnologia – gli elementi centrali della competizione intersettoriale. Sono la vera opportunità di fronte alla sfida.

Bigtech e intermediari finanziari condividono in pieno l'elemento della fiducia; la sfida è quindi far divenire il *trust* da vulnerabilità percepita ad *asset* competitivo. Gli intermediari finanziari e le *infrastrutture di mercato* da sempre vendono sicurezza, *sub specie* di sicurezza economica: non ci sono ragioni perché non possano vendere anche la nuova sicurezza. Come avviene per altri settori economici sensibili, chi investe per la propria sicurezza acquisisce un *know how* ed una capacità che può essere messa a disposizione dei propri clienti. In alcuni ambiti di innovazione finanziaria, ciò sarà indispensabile: si pensi alla necessità di garantire la sicurezza logica di protezione delle chiavi di cifratura dei *criptoasset* detenuti in un *wallet*, virtualmente connesso allo *smartphone* del cliente.

La nuova sfida che deriva dal regolamento DORA richiede che l'offerta di servizi di sicurezza *cyber* per il sistema finanziario italiano sia adeguata alla domanda che a breve si presenterà. Allo stato mancano attori nazionali alla scala dell'impegno che si va delineando. Il dato informativo da proteggere riveste un carattere sensibile ed una riflessione settoriale potrebbe essere utile.

Più in generale, le sfide che la rivoluzione dei dati pone al sistema finanziario nazionale e globale sono tali che solo un rapporto stretto con la ricerca, quella di base in particolare, permetterà di dare risposta alle molte domande che già ora si presentano. Alcune sono comuni al sistema finanziario nel suo complesso, altre sono diverse tra settore bancario e settore finanziario. L'Unione a breve presenterà numerose iniziative legislative in materia di *data governance* con l'ambizione di creare uno spazio comune europeo dei dati: in questo nuovo quadro, emergerà la necessità di posizionare le opportunità per il sistema finanziario italiano. In questo senso, occorre una messa a sistema delle capacità di ricerca nazionale in campo di innovazione tecnologica per la finanza. Il regolatore finanziario, la Consob, che ha da tempo avviato questo sforzo e da ultimo con il Politecnico di Milano, può certamente svolgere una funzione di *honest brokerage* per accelerare questo processo.

*** * ***

Come disse John Fitzgerald Kennedy nel suo discorso a Indianapolis del 12 aprile 1959, a proposito del termine cinese *Wēijī*

When written in Chinese, the word "crisis" is composed of two characters - one represents danger and one represents opportunity

Ora certamente sapete anche del dibattito che si è aperto tra i linguisti sulla corretta traduzione in particolare della seconda parte del concetto. Ma, discussioni linguistiche a parte, io sono certo che questo è un momento di trasformazione, di transizione a un nuovo stato: siamo a un punto cruciale, sta a noi coglierne l'opportunità e trasformarla in un successo. Al *Bing Bang* regolatorio comunitario deve accompagnarsi un *Big Bang* nazionale di investimenti in *start-up* e ricerca di base, a sostegno di innovazione e sicurezza, che sia di stimolo per crescere e far crescere.

Grazie.