Data and finance: new opportunities and new vulnerabilities.
The need to change paradigm

Paolo Ciocca
Consob Commissioner
Rome, November 18 - 2020

Good morning.
I thank President Patuelli, General Manager Sabatini and all of you for the opportunity to be here with you today.
It is a real personal pleasure for me to return to address the Association, where I had the opportunity to work eighteen years ago, on issues other than those we will discuss today. But the perspective that comes with age and with different professional experiences makes me think that perhaps this distance is only apparent.

CMU, technological revolution, European and global competition

The Commission recently presented its roadmap for the CMU (Capital Markets Union). This is an important project that aims at an ambitious result; I would say it is essential for the European market to be up to the global post-Covid and post-Brexit challenge. We need a deeper and less fragmented regional financial center to satisfy the thirst for equity of our companies that want to grow and seize the opportunities offered by technological innovation. It is therefore no coincidence that the Commission's program presents ESAP (European Single Access Point) as its first short-term objective, namely the creation of an information "infrastructure" that acts as a single access point to the information compendium - financial and otherwise - of issuers, including on sustainability, in order to facilitate the comparison of data, the cross-border visibility of our companies and the allocative efficiency of EU markets. The project is complemented by recent legislative initiatives on digital finance, which provide substance to the CMU. The regulatory preconditions are therefore established so that the Union can fully respond to the competitive challenge that comes from both West and East in this field.

But in the meantime the market is moving: let's think of the recent Euronext / Borsa Italiana and LSEG / Refinitiv transactions. All in all, we are witnessing, on the one hand, a regional (horizontal) consolidation of important market operators, which makes the CMU real. On the other hand, a (vertical) consolidation of business segments united by the use and enhancement of financial big data. In this second case it is evident the ambition to create a global player that takes full advantage of the integration between different data sources.

This is clearly a global competition, on a highly sensitive terrain - that of data and the infrastructures on which they pass; when it comes to data, national (and regional) security is (are) a necessary and unavoidable element. As we will see later, the intersection between national security and EU security is not easy to decline, so new approaches are needed.

Digital enabler technologies: but which ones?

What innovative technologies are we talking about? Many of the applications are well known: roboadvice, algotrade, customer profiling just to name a few of those employed in the front office of intermediaries; or AML and anti-fraud automated analysis, for those in the back office. All new applications are generally attributable to some fundamental technologies: Cloud Computing, DLTs, Big Data & Machine Learning, Artificial Intelligence.

Cloud Computing is certainly not a new technology as it now widely pervades the global IT market. Covid-19, forcing the global use of remote work, has highlighted the infrastructural nature of this service, which represents the premise - the playing field - in which the other innovations reside. Driven by the economic and architectural efficiency for corporate IT infrastructures, Cloud Computing profoundly changes the map of opportunities and risks of intermediaries and supervisory authorities, and determines outsourcing with centralization of both data and processing, even the most sensitive ones. On the supply side, there is no single large European provider that can compete on a global scale. Hence the importance of the recent EU Gaia-X initiative, which seeks to subsidize this absence with a public / private partnership. This initiative is based on strong regulatory coordination, rather than on an artificial (and unlikely) hypothesis of creating an EU Bigtech from scratch. In this regard, the recent EU proposal of DORA (digital operational resilience) regulation represents the right answer with a unitary EU financial market framework for the supervision of major cloud providers (by both European and national regulators), with outcome-based objectives - rather than just compliance - for both financial intermediaries and authorities. This will not be enough: for the European region to effectively compete in the global confrontation, a convinced participation in European initiatives, such as Gaia-X, will be necessary, by both market as well as European and national public authorities.

DLTs are progressively making their way, especially in back office, with their ability to provide reliability of transactions through a decentralized and shared control system. Consob, with its in-depth analysis - first on ICOs (initial coin offerings) and now on STOs (securities token offerings) - has acquired considerable regulatory know-how. In this sense, the time is approaching to share a reflection on the most appropriate ways to regulate the issuance of securities through DLT technologies, also in light of the growing demand from market players. The advantages, in terms cost of issuance reduction, are important. The regulator must focus on substantive guarantees to be provided to subscribers, both in terms of circulation and liquidity of the securities. The recent proposals for EU regulations MICA (markets in cryptoassets) and PILOT (pilot regime for market infrastructures based on distributed ledger technology), by fully confirming the preliminary analysis of Consob, represent an important step forward for the achievement of a digital financial market: MICA provides for the definition of cryptoassets which are not financial instruments; PILOT paves the way for experimenting a secondary market for these instruments. These new assets will be able to circulate freely in the EU market and Italy is certainly a target market: in light of this, during the negotiations that are being conducted, there is the need to pay the utmost attention to prevent weakening MiFID protections, while supporting innovation. Issues around definitions and the level of harmonization conditions related to internal market access will be crucial.

Big data and advanced analytics: the real revolution lies in the availability of a huge amount of data, financial and otherwise, to be analysed and processed through predictive algorithms. The circuit is well-known: data, information, knowledge, wisdom. The most relevant are the technologies based on machine learning, which allow to process (i.e., collect, compose, extract, sort, cross, correlate, etc.) these immense amounts of data. We are still in the field of - albeit elaborate - techniques; accelerations are important in both financial and non-financial areas. For example, whilst for the time being robotics is not a crucial element for the financial sector, the same certainly cannot be said for facial recognition techniques: the latter, created to respond to public order needs, are finding full application in the financial field in China. As regards machine learning, the most advanced research touches upon very relevant issues, also for the financial system, such as the ability to extract correlations between databases without the need to know the plaintext content of the same, or the ability to evaluate ex ante the potential advancements of the same algorithms.

More generally, in the field of artificial intelligence, progress is moving forward very quickly, while the time required for the development of reliable technologies for the direct machine-to-human connection is short; and here the story is still to be written.

This is the area that poses the most important challenges for intermediaries and regulators.

Some out of the many: how to control the activity of highly sophisticated and self-learning algorithms (and for which it is not possible to predict the evolution of the activity) which - by definition - cannot be analysed ex ante?

The principle of machine learning is based on an algorithm to learn from a data set to be subsequently applied live: how to avoid the bias (of any kind) that can derive from the limits of the learning base?

Think of the reputational risks for an intermediary of a bias in the algorithm and not understood until the effects occur, for example in the lending processing, or in customer profiling. Furthermore, since it is not an ordinary software - for which one could in the abstract invoke a responsibility of the supplier - here the algorithm develops and refines its analysis and choice skills (perhaps incorrectly) only within the systems of the single intermediary, with all the due consequences.

These challenges, many of them cross-industry, are currently being studied by data science, and the results of these studies will certainly also be crucial for the activity of regulators and intermediaries. The financial industry is at the forefront in the development of these technologies, and investments in the financial sector are certainly among the most substantive.

At the same time - and even more so - there must be full awareness by the banking sector of these (new) risks. Awareness must also pervade the corporate governance of the individual intermediary at all its levels: the tone from the top is essential.

The continuous relationship between industry - individual and associated - and research is fundamental and represents the strategic keystone for facing the revolution.

Where are the Bigtechs positioned?

One could say: are these problems the same that a non-financial Bigtech must face, who is the one using these technologies as first (and possibly best)? Here what counts is the different degree of regulation of the two sectors, data and financial, and the different attitudes by market players. On the one hand, financial intermediaries - incumbents and innovative natives - who are facing the progressive application of technologies, on the other hand Bigtechs showing up in the financial sector. It seems to me there is an opportunistic approach by Bigtechs in entering business segments in which: i) technology is predominant; and ii) the (perceived) reputational risk is lower. Hence the growing interest of Bigtechs in the payment system, rather than in core services (lending or issuing of financial assets).

Two short digressions.

The first is of a global nature. This picture applies to the Western financial system, whilst the situation in the East is quite different: the Chinese financial ecosystem, through superapps, allows local Bigtechs to offer a very wide range of financial services directly to customers. The effects of disruption, including architectural disruption, are evident given the recent institutional tensions that emerged on the occasion of the planned (and then withdrawn) IPO of Antfinancial. The testing of core services takes place in markets where economic conditions and less stringent rules facilitate these processes; and these players will therefore soon find themselves ready to make the leap into more advanced markets.

The second is rather of method: the determining variable of this competitive equation between the two sectors is certainly time. If the time given to the financial sector to prepare for the challenge had been shortened up to now, as a result of Covid this time is essentially over. The isolation caused by the pandemic has benefited those actors exploiting network effects in their production model, Bigtech in particular. An easy prediction is that the post-Covid competitive scenario, particularly in the financial sector, will record an advantage for unconventional players and able to exploit the network effect.

I return to the main point, to conclude.

This "external" competitive pressure must stimulate traditional operators to innovate more and more quickly, exploiting the enormous wealth deriving from their own information assets and the opportunities offered by data sharing at EU level, through investments and collaboration with the Fintech world. Now or never.

An old concept in the new world: **trust**

But the world of data and finance certainly have both something in common: trust. This applies both industry-wide as well as individually. The effects of the crisis of confidence in the financial sector are quite obvious; just as important are the same crisis for Bigtechs (FB among all). In the financial system, trust is the result of a complex set of factors: financial stability, reputation, security among others.

I will focus on the safety aspect. Cybersecurity does not equate to IT security. The concept is a much broader concept and takes into account technological, economic and geopolitical context.

Technological context: the acceleration of innovation, the enormous expansion of the network connection , the prospects of a complete IoT connection, the ongoing data sharing on technological platforms. According to a basic security canon, an expansion of the attack surface results in an increase in vulnerability. Depending on the context, the increase can be even more than proportional. A cyber attack is traceable (in IT terms) with extreme difficulty, and only in a few cases in real time. At the same time, the cyber tool has infinite operational flexibility. Finally, in a system based on network connections, even the last link in the chain can trigger a vulnerability for the whole system.

Economic context: technological acceleration is associated with ever greater portions of added value, both at a macro and micro level. This leads to a growing interest by the hostile actor, traditional (thief, terrorist, etc.) or State one.

But there is also the sum of the two: the availability of new "weapons", of new complex malware at a very low price with effects of exponentially increasing the risk. For an hostile actor, what matters is the impact value: e.g. a malware that leads to the blocking, even if only partial, of a main financial infrastructure such as a stock exchange; the actual value depends on the perceived impact, and the markets are connected (e.g. a regional stock exchange system); given the centrality of the financial system in the overall economy, the ultimate impact value is even greater; finally, in a social information context, the impact value can easily be amplified through disinformation.

There is also a geopolitical component. The (technical) difficulty of attributing attacks entails the absence of clear rules, recognized by the international community, aimed at sanctioning hostile behavior. This, together with the high profitability of the cyber attack, has determined a structural change in the risk / opportunity equation and in the concept of deterrence itself. Strategic analysis has now unanimously identified what represents in all respects a state of undeclared conflict, below the internationally recognized level of the act of war (which gives the right to a proportionate response); and this conflict takes place (almost) exclusively in a non-military terrain.

The financial sector, due to its strategic centrality, is at the center of this conflict.

These considerations have an effect for the financial system, its infrastructures and for individual intermediaries.

The technical difficulty in the attribution of cyber attacks does not mean that States do not have other tools to attribute an attack and to understand the actor and reasons behind (who & why). But only the Government

has the overall picture of information / factors (the DIMEFIL matrix) behind a cyber attack. Therefore, the relationship with the Government - with its national security and law enforcement bodies - becomes a crucial element, especially in the most complex situations.

Equally fundamental is the attitude of management at all levels, of the Board of Directors, of the supervisory bodies. Here, too, the tone from the top applies. It is a question of evolving from compliance (tick the box attitude) to resilience: it is not a question of if, but of when and how. The intermediary and the financial infrastructure must therefore choose their own defensive posture with respect to a framework which, subject to the necessary minimum, defines the level of protection that the organization aims for through a process of aware choice taken by the various corporate bodies.

Given this, the fundamental nature of the proposed EU DORA regulation is perhaps now better explained: a cyber security Big Bang for the EU financial system with common challenging objectives. With the effect of instantaneously raising the regional standard, which makes the EU financial system stronger and has global repercussions: similar - albeit on a different ground - to the effect then implied by GDPR. And with a very timely choice of time, i.e. close to Brexit.

During the negotiation of the regulation, an issue that will certainly require further analysis is the intersection between the EU competences of the supervisory bodies (national and EU) and national security issues, which currently remains in the exclusive competence of Member States. This is a field still to be explored.

Some initial strategic reflections for the Italian financial sector

The President of the Republic at the annual Consob meeting, last June, recalled that "*the role of the market is central in the recovery process of a country that has suffered an unprecedented health crisis, with serious economic and social effects, and consequences that are still difficult to assess in their complexity*".

From Covid-19 we all will come out different, individually and in our respective institutional and corporate roles. As for today's theme, I have already said: the time to seize the opportunity for transformation is over.

In my opinion, the national financial system must fully embrace the technological revolution leveraging - in view of the cross-sector competition - on its strengths, such as the breadth of the information content collected in one's business, the natural ability to interconnect between the various intermediaries, the current and future dimension of investments in technology. These are the real opportunities in the face of the challenge.

Bigtech and financial intermediaries share fully the element of trust; the challenge is therefore to transform trust from a perceived vulnerability to a competitive asset. Financial intermediaries and market infrastructures have always sold security, i.e. economic security: there is no reason why they cannot sell also the new security. Similar to other sensitive sectors, firms who invest in their own safety acquire know-how and skills that can be made available to their customers. In some areas of financial innovation, this will be indispensable: e.g. the need to warrant protection of logical security when it comes to the encryption keys of cryptoassets held in a wallet, virtually resident on a customer's smartphone.

The new challenge arising from the DORA regulation requires that the offer of cyber security services for the Italian financial system is adequate to the demand that will soon arise. At present there is a lack of national actors on the scale of the emerging commitment. Data to be protected is of a sensitive nature and a sectoral reflection could be useful.

More generally, the challenges that the data revolution poses to the national and global financial system are such that only a close relationship with research, in particular basic research, will allow an answer to the many questions that are already arising. Some are common to the financial system as a whole, others are

different between the banking and financial sectors. The Union will shortly present several legislative initiatives on data governance with the ambition of creating a common European data space: in this new framework, the Italian financial system needs to seize the emerging opportunities. It is necessary to organize a national research capacity in the field of technological innovation for finance. The financial regulator, Consob, which started this effort some time ago and most recently with the Politecnico di Milano, can certainly perform an honest brokerage function to accelerate this process.

* * *

As John Fitzgerald Kennedy said in his speech in Indianapolis of April 12, 1959, on the Chinese term Wēijī

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

Now you also know of the debate that has opened up among linguists on the correct translation of the second part of the concept. Linguistic discussions aside, I am sure that this is a moment of transformation, of transition to a new state: we are at a crucial point, it is up to us to seize the opportunity and turn it into a success. The EU regulatory Bing Bang must be accompanied by a national Big Bang of investments in start-ups and basic research, in support of innovation and security, which is a stimulus for growth.

Thanks.