BBVA CONTRIBUTION TO ESAs JOINT COMMITTEE CONSULTATION ON THE USE OF BIG DATA BY FINANCIAL INSTITUTIONS

DESCRIPTION OF THE PHENOMENON

1. **Do you agree with the above description of the big data phenomenon? If not, please explain why. Please, also mention whether you consider that other characteristics are relevant to understanding the use of big data.**

    - Algorithms can be built upon small data as well. Hence, it could be better to talk about Data Science instead.
    - As for the types of firms using big data mentioned by the ESAs in the description of the phenomenon, another type should also be mentioned besides traditional financial services firms, new fintech startups and pure digital players, especially the larger ones (so-called Big Techs). There are certain sectors which are also highly impacted by the use of data and big data technologies, sectors that are also data reliant, like the telecommunications or energy sector. Telecommunications operators also perform an intensive use of data and some of them are starting to integrate financial services into their portfolio.
    - An important element to highlight regarding the description of the big data phenomenon is that big data mostly works with anonymized and aggregated data, in order to ensure the protection of privacy and to comply with regulations. Another important element for big data is the possibility to combine datasets from many different sources, as to derive more (and new) information.

2. **Which financial products/activities are (likely to be) the most impacted by the use of big data and which type of entities (e.g. large, small, traditional financial institutions, fintechs, etc) are making more use of big data technologies? In light of ESA's objective to contribute to the stability and effectiveness of the financial system, to prevent regulatory arbitrage, do you consider that there is a level playing field between financial institutions using big data processes and those not using them (e.g. because they do not have access to data or the (IT) resources to implement big data processes) or between established financial institutions and potential new entrants (e.g. Fintechs) using big data processes? Please, explain.**
    - All those activities that have been digitized and, as such, can be systematized, will be most impacted (from credit valuations to trading strategies). Internally, the game changer is that the knowledge of the demand for a product or a service (its elasticity included) has shifted from fuzzy, non-shareable memories in our staff to clean, shareable attributes in a database. Further knowledge can now be discovered by any unit, in an isolated manner, with access to all required information. Traditional, large financial institutions have the largest challenge when it comes to dealing with legacies (whether tech or human) when adapting themselves to the data-driven ecosystem. The smaller ones may have issues when finding

resources to face the data-related costs. But typically, it is easier to find an incremental budget than to make large internal changes.

- The ones using more big data are not actually financial players. The financial sector is not the only sector using big data, and other sectors using it like Telco, Energy or Service Providers such as Facebook, Google and Amazon are going to come into play in the financial sector (sometimes due to the help of regulators forcing European Account Servicing Payments Providers to open their data to third parties via PSD2), and the contrary is very unlikely to happen, unless the financial sector reaches punctual agreements with individual companies in specific sectors. For example, in Belgium the banking sector has agreed on an alliance with telcos to share identity data that could benefit both in the onboarding of new customers in a fast and compliant way.
- Most fintechs, telcos or digital service providers are not subject to financial regulations and are therefore less constrained in their use of big data. These players are clearly in advantage and no regulation is forcing them to share their data openly (as PSD2 does). This is creating an unlevel playing field for those financial institutions subject to regulations that force them to share data one way only.
- We embrace the fintech phenomenon at a broad level, we have actually partnered and investede in a number of companies and think that new entrants could benefit our sector and improve overall customer experience.
- Taking into account that financial services have no physical production or logistics processes *per se*, but are rather fueled by a huge number of real-time transactions, backed up by a massive amount of historical data to support decision-making, the potential of big data is enormous. Some of the most impacted areas or products are risk management, where big data can promote more accurate risk estimations at a lower cost; or personalised marketing, allowing financial institutions to collect and analyze customer data and provide tailor-made services. Security, fraud management and regulatory compliance are other areas that can be improved due to big data technologies. Financial institutions know their customers' behavioural patterns in terms of payments, consumption, propensity to save and invest, risk aversion, etc, and there is a huge potential to improve customer experience thanks to the extraction of value from that knowledge. Financial institutions face strong rules as regards security, privacy and confidentiality, which may go far beyond what is expected from a general private enterprise. Moreover, financial institutions often go beyond what is strictly required by Law, as reputational risk is a relevant factor to be considered. Authorities must ensure that their supervisory approach produces financial stability and establishes a level playing field for banks and technological innovators (either Fintech startups or technological giants). It is desirable to follow a risk-based approach, following the principle of "same business, same risks, same rules".

3. **Do you offer/are you considering using big data tools as part of your business model? If so, please briefly describe: i) what type of entity you are, e.g. long established, start-up, a product provider, an intermediary, ii)**

the service you provide; iii) the nature of your clients; IV) your business model; V) whether the big data tools/strategy were developed by an external company or internally and whether you have related agreements with other entities (including non-financial entities); VI) what are the types of data used (personal, anonymised, user data, statistical data, etc); VII) the size of your big data related activity and/or forecast activity (e.g. to what extent are business decisions already taken on the basis of big data analysis; what other business actions could be based on big data in the future)?

4. **If you are a consumer or consumer organization, do you witness any of the uses of big data? In what fields?**

5. **Do you consider there are (non-regulatory) barriers preventing you (or which could prevent you in the future) from collecting and processing data? Are there barriers preventing you from offering/developing big data tools in the banking, insurance and securities sector? If so, which barriers?**
    - IT risk barriers: banking IT platforms are expensive, hence scientists in large financial institutions cannot freely try out different technology stacks. Moreover, whichever IT plan is agreed at a certain point in time becomes instantly a legacy for several years to come. This is not the case in smaller financial institutions or new entrants. This adds frustration to the data scientists, who could have a higher churn rate at large financial institutions, since they move around the industry looking for the best platforms to develop/update their skills.

REGULATORY FRAMEWORK APPLICABLE TO BIG DATA

6. **Do you agree with the above short, non-exhaustive, presentation of some of the main applicable requirements? If not, please explain why. Please also mention whether you consider that other legal requirements are essential and should be mentioned.**
    - We generally agree. Nonetheless, in relation to specific financial regulation, financial supervisory regulation on outsourcing should be mentioned (Circular 2/2016, 2 February, Banco de España/Directive 2013/36/EC). Indeed, many big data solutions are based on cloud technology. Regulatory and supervisory authorities (with certain national discrepancies) require prior notification of outsourcing (cloud is a type of outsourcing), which in practice sets an approval prerequisite to migrate workloads to the cloud. Authorisation must be granted for individual projects. This increases time to market and delays innovation and it can pose barriers to the use of big data technologies by

banking institutions. Moreover, this can be an example of lack of level playing field with other players.

- The achievement of an adequately[1] regulated - and supervised- level playing field covering all kinds of activities and products from a sector-neutral perspective is of the utmost importance. It will contribute to bolster the benefits of big data while mitigating the negative consequences derived from regulatory arbitrage that concedes advantages to some of the players.
- As for footnote number 29, the reference to explicit consent is not complete. According to the GDPR, the situations under which explicit consent is required are more than those mentioned in footnote number 29. Moreover, it would be relevant to deepen into the legal grounds, among others, of legitimate interest for personal data processing. Also, with regard to the reference to profiling purposes *"new provisions on profiling allow, subject to certain conditions, the data subject to unsubscribe/opt-out from decisions based on profiling"*. We should take into account that the data subject can oppose to profiling for direct marketing purposes, while automated individual decision-making must be based on either explicit consent or if it is needed for the execution or performance of a contract.

7. **Do you consider any of these regulatory requirements as unjustified barriers preventing you from using big data technologies? If so, please explain why. Please also explain whether you consider that further regulation (including soft law/guidance, etc, and insofar as it falls within the scope/remit of the ESAs) should be introduced to facilitate the use of big data technologies.**
    - Privacy and data protection issues should be ruled by sector-neutral regulations, hence there is no need for specific regulations for the financial sector. The new GDPR already reinforces significantly personal data protection in the EU. Some requirements established in the GDPR could be understood as barriers to the use of big data, in particular those related to the duty to inform data subjects regarding the specific purposes. In many cases, data scientists will discover new possible uses beyond the initial scope of a certain big data analysis. A stringent interpretation of information duties might exclude this possibility, preventing the data subject from receiving additional benefits derived from those new possible uses. Also the new conditions introduced for consent, with more stringent requirements and the prohibition of tacit consent can be understood as an indirect barrier to big data.
    - If further regulation is introduced to facilitate the use of big data technologies, avoiding overlappings and inconsistencies with already existing regulations is key. These include GDPR, PSD2, the Mortgage Credit Directive, the Consumer Credit Directive, the PAD, PRIIPS, the Insurance Distribution Directive, MiFID II, MiFIR, UCITS, AIFMD, EMIR, Solvency II and CRD IV[2].

[1] It is our understanding that having the adequate requirements is more important than having a lot of requirements. An excess of regulation can limit innovation and can be a significant barrier to entry.

[2] i.e.: The CRD IV, AIFMD and UCITS advocate for a solid internal governance, a prudent risk management and strong internal control mechanisms. Under MiFID II, it has to be guaranteed that trading systems are correctly

Overlappings and inconsistencies between different pieces of regulation mislead consumers -instead of protecting them- and can imply unnecessary, non-negligible burden for entities in terms of human capital, time and money as a consequence of an inefficient allocation of resources. For this reason, we should bear in mind that if further regulation is introduced, we should avoid overlappings and pursue simplification. Last, but not least, if new regulatory requirements are introduced, the proportionality principle should be considered whenever possible. That is, systems, resources and procedures have to be adequate to their associated risks and to the complexity of their final goals.

- The EC has launched an initiative, still in the phase of consultation and dialogue with stakeholders to evaluate the best possible solution, to analyze the possibility of developing a regulatory framework for data-related issues. These include data ownership, liability, portability and standards, for non-personal data and machine-generated data in the context of IoT (Internet of Things) or autonomous systems, which are closely related to big data. Any future development in this field should be taken into account.
- In the case of deletion of data which may have been used for profiling, it would be convenient that the user is informed of the implications of the removal of his/her digital footprint. This removal of profiling data could be used to the advantage of the consumer (for example, the right to be forgotten applied to bad credit history). However, on the opposite side, it could also be a disadvantage for the user. For example, a person who has no financial history when applying for insurance or credit has a higher negative risk scoring than one that has history data. The reason is that the data may show that the customer has sufficient capital for a credit and no due receipts or any bad records. Therefore, the importance of maintaining history big data should be considered beneficial for the customer, just as data used in a medical record can help diagnose diseases, suggest new treatments, etc. Obviously, there is a need for transparency and confidentiality, but in the future, data will increase the digital footprint of the user. Social media are already creating this profile based on user interactions. It is well known that with the rise of global networks, information flows from one place to another, once it has been published on the Internet. Provisions included in the GDPR, like the right to be forgotten, could imply a barrier to the use of big data technologies, if applied in a very restrictive manner.
- We see a problem with security obligations like anonymization and pseudonymization. There is an associated cost related to these procedures and there are also software-as-a-service (SaaS) solutions and products that are not currently built to comply with these techniques. These products and services are often provided by American companies subject to different regulations and that target their national market primarily. For example, there are products and services that encrypt using their own libraries and private keys, not allowing for the data owner to use its own. Besides, some

tested and monitored; furthermore, firms are subject to multiple requirements for pre-trade and post-trade transparency reporting.

companies could be discouraged from offering big data services in Europe due to a stricter compliance with security and privacy rules.

- We see the e-privacy Directive (e-Privacy Regulation in the near future) as a complement to the GDPR, and both of them are good steps towards protecting privacy and security, but we still think there is much more that can be done in regards to avoiding data breaches. Notification is a good step forward to get regulators involved and those to be able to notify governments, but there is still a lack of action in the following scenarios:

  -Regulators and supervisors are notified about breaches under the following regulations: Data Protection Law, Critical infrastructure Law, Payment Services Directive 2, Network Information Directive, or the forthcoming European Central Bank incident reporting. There is no feedback provided to the rest of the financial community. For example, a phishing campaign provoking data breaches is notified to the different regulators and supervisors mentioned previously, but none of them informs the rest of the financial institutions that there is a phishing campaign going on, with all the necessary information to react accordingly in case they are the next in line. In this sense, cyber crime is taking advantage of a lack of coordination among the financial community.

  -There is also a lack of legal coordination when a financial institution tries to prosecute a large botnet where all the IP addresses of users involved come from different countries spread around Europe and the world. The different jurisdictions and the complexity of the forensic and legal processes make it extremely difficult for the financial sector to respond adequately.

  -End users who are infected by a phishing campaign due to their lack of knowledge, inability to have a minimum protection like an active antivirus and firewall are not responsible if they are hacked. It is the responsibility of the financial sector to assume the fraud and pay the customer back. This scenario with the increasing usage of the IoT, smartphones, smart tv or any device capable of making payments is going to increase data breaches. Security education is only part of the solution, and it only reduces the risk. New techniques based on the patterns of the end users need to be captured in order to detect anomalies, and this big data would need to be processed in order to detect possible frauds and attacks.

- In regards to the quality and continuous performance of outsourcing, the track record of the financial industry (and in comparison to other industries) has been outstanding. Partly because this sector has always been the first to adopt new technologies to serve its customers, create loyalty, privacy, and security since its very origins. That is why banks are so secure and have the best technology and processes to secure their systems, their clients' wealth and Know the data which also holds great value. If a bank decides to outsource its data or systems, they need to comply with the same security, privacy, cost and business prerequisites as if they were creating an extension

of their data center or a new backup of it. Because, in our business, there is still the basic need to maintain trust via security. However, the process of outsourcing should also be lean in regards to communicating all the necessary information to the regulators and supervisors so as to minimize the lifecycle of a new solution to, for example, a cloud service provider. The key is to comply with the necessary elements to justify internally and externally the necessary due diligence and audits of this cloud service provider. And once it has been cleared out by the corresponding supervisor and the financial entity, the subsequent usage of the same cloud service provider, as long as there have been no significant changes in the provider or the financial service, should be as lean as possible.

POTENTIAL BENEFITS AND RISKS FOR CONSUMERS AND FINANCIAL INSTITUTIONS

8. **Do you consider the potential benefits for consumers and respectively financial institutions to be accurately described? Have you observed any of them in practice? If so, please, provide examples. If not, please explain whether you are aware of any barriers that may prevent the above potential benefits from materialising.**
    - Consumers do benefit from data science and big data through several dimensions. Internal *efficiency* from a bank perspective is directly translated into more affordable prices for customers. *Immediacy* when responding to clients' queries allows for a timely response to the customers' needs (eg fast scoring -> fast pricing -> fast comparison across financial services providers -> fast funding not to lose competed opportunities). *Discovery* of sub-optimal states in the financial wallet of our clients (eg by tracking the value of real estate owned by the customer and comparing it with the total amount for which it has been insured the client can be alerted from undesired deviations).
    - Financial inclusion can be promoted not only due to the use of more detailed information derived from the use of big data, but also because of the use of alternative sources of data, using non-traditional sources of data and methods that can benefit consumers that otherwise would be unscorable.
    - Big data can increasingly improve customer experience. This customer experience improvement might be more evident in retail banking. Every engagement with the customer can be translated into an opportunity for both the company and the customer. Better understanding the customer, how she likes to communicate or her preferred services help organizations to offer the product their clients need, at the right time. It can enable organizations to anticipate which services or products customers will be willing to consume. It enables to identify customers with long term profitability potential and proactively make contextually relevant offers. Dealing with information, for instance, like spending and income patterns or geographical location, enables

organizations to have a clear picture of their customers, which is then translated into a better and more agile service.

- Big data can also contribute significantly to operational efficiency and makes it possible to break down data silos and provide a comprehensive holistic picture of operations. Big data solutions can enable companies to address their operations in an interconnected ecosystem, as opposed to a collection of isolated departments. A big data and analytics implementation can help organizations uncover ways to make operations more efficient and effective by improving asset efficiency and streamlining operations, while automating decision making. In order to be able to deal with unexpected changes like, for instance, shifts in customer behaviour, predictive models that can be built on different kinds of data can monitor and adjust to changing circumstances.
- We could take this opportunity to highlight why certain risks and potential benefits could seriously disrupt the financial sector:

  -One of the motivations underlying PSD2 was opening the financial services sector to more competition. However, there are other non-financial players with access to large datasets and big data knowledge to exploit them. Access to these datasets could also be of interest to other sectors for the benefit of consumers. For example, the data held by the telco or energy sectors, both personal and non-personal, are of high value too. Big players such as Amazon, Google, Facebook, the public sector or the telco industry hold a lot of data which, if properly unlocked for other players, just as PSD2 is opening account information, both as regards personal and non personal data, could trigger innovation, transformation and ultimately benefits to consumers. If other types of non-financial data were subjected to the same fair rules as PSD2, then we would be contributing to a level playing field in the big data space, helping Europe become more competitive.

  -Too much control over the protection and privacy of big data could restrict its full potential, especially when analyzing or profiling data. The use of encryption should be sufficient for most cases in which highly sensitive data needs to be processed. However, special consideration should be taken on certain Cloud computing solutions and services (for example SaaS) that need to consider in their functionality the control of the private keys by the Cloud user or customer, for encryption, instead of cloud providers having its control. Besides, security solutions that aim at keeping personal data encrypted or protected in non-structured and semi structured environments are difficult to implement when handling large amounts of data. Consequently, other alternatives should be taken into consideration, including access control or monitoring. This is one of the reasons why more attention should be paid to the big data processes needed to comply with security and privacy regulations and why Chief Data Officers are on the rise.

- More granular risk segmentation could lead to higher premiums, as it has been occurring before the digital era, so this is not a new issue affecting customers. Before, in the predigital era, information was gathered in an analog way with less information or with more time needed to segment or take a decision. Today, new digital ways and data have helped create faster, more affordable and smaller segmentations, but this phenomenon and the consequent constraints on access to credit for certain customers has been happening since the origins of credit. Moreover, the transparency applied back in the day holds the same principles today. Market competition and the laws of supply and demand can provide a customer insurance. A company that does not offer an insurance to one customer may be an opportunity for another company to offer insurance to the same customer. In regards to the statement *"certain consumers could be left out of these clusters, for example if they refuse to share their personal information with financial institutions"*, this holds true since the early history of insurance. A customer that for example refuses to provide information about his health, driving experience age, or provides false information to a car insurance company will not be insured or will only be covered if paying higher premiums. A basic set of information is needed and it is important to understand that this should not be considered discrimination, as some customers may not be in conditions of driving or might put at risk other drivers if the insurance is provided.
- Point 42 seems to suggest the need to standardize products and services so consumers can make better decisions. We think this is highly risky, controlling the market forces could lead to less competition and innovation. In the absence of regulation, innovation by new entrants could also provoke the creation of aggregation services that compare products and services from different financial or insurance companies. There are already some of these companies providing this service and we are sure that this trend will grow as data becomes more open and shareable between companies.
- Point 44 and 55 describe possible negative scenarios, but in any case they should be mitigated by compliance with actual EU regulations, such as the ones cited in the footnote. Nevertheless, we prefer to view the usage of history data, sentiment or behaviour data as a new way to promote new and better digital products in Europe. The Digital Single Market can only be achieved if data flows are allowed and the data-driven economy becomes a reality. We see that there are still many sectors that could potentially help to promote this new digital economy by sharing data more intelligently and obviously under the strict requirements of privacy and security laws.
- Point 52. The discovery of phishing activity is happening without the need of big data. A more accurate concept would be "fraudulent activity", which goes beyond phishing campaigns and that could help detect other types of attacks such as the ones mentioned in regards to the impact on the reputation of the company. big data can make use of social media to detect certain sources of fraud but it is more efficiently used with internal big data. This approach detects, for example, fraudulent transactions by seeking uncommon patterns

such as a person making a physical purchase in Hong Kong and paying for dinner a few minutes before in London.

- We agree with the e-skills challenges posed and this issue definitely requires education and training. However, assurance is already part of the ICT compliance to current regulations and laws coming from regulators and supervisors. Indeed, this is vital for the survival of the company as errors go in detriment of the company's image and trust. The EU could help in this regards by promoting and incentivising this type of e-skills in schools and universities. There is an e-skill program in the EU but it seems more directed to the public sector than to the private one. Nowadays, most of this new skills such as data science are recycled data or scientific personnel who need to be properly trained by their company.
- Point 69. Yes we are aware of the GDPR, but the GDPR is only focused on personal data, while big data deals with other types of data. Some big data is not considered as processing personal data; other types are not even in the realm of GDPR because the data does not belong to European residents.
- Point 70. That is why using artificial intelligence, machine learning or other types of algorithms over certain big data can help us prevent certain cyber attacks or frauds. We base this analysis on patterns but also on a risk-based approach which can help mitigate different scenarios from insider attacks or inappropriate use of data to external cyber attacks. The more it becomes automatized without human intervention, the less risk and the faster response time. Moreover, we will also have the possibility to do better forensic analysis which we could provide to third parties such as regulators/supervisors or even to other institutions in order to help them avoid a future fraud or cyber attack.
- Point 73. This is a decision that the consumer must make, to leave with more Internet of Things or robots that can enhance their life experience or not. They can always opt-out or decide not to use them or shut them temporarily. These questions have risen in the past during the dawn of the industrial revolution and the results are well known. Nevertheless, we need to understand the importance of this new industrial revolution and that there is a need to protect and inform the most vulnerable consumers.

9. **Do you believe that big data processes may enable financial institutions to predict more accurately (and act accordingly) the behavior of consumers (e.g. predicting which consumers are more likely to shop around, or to lodge a complaint or to accept claims settlements offers) and do you agree with the description of the risks identified for consumers and respectively financial institutions? Have you observed any of these risks (including other risks that you are aware of) causing detriment to consumers and respectively financial institutions? If so, in what way? If not, please, explain why. Please also mention whether certain risks for consumers and financial institutions have not manifested yet but have the potential of developing in the future and hence need to be closely monitored by Supervisory Authorities.**

- Aggregators could mitigate many of these, especially if prices are systematic at financial institutions. If that is the case and there is the possibility for the aggregator to request a quote on a product/service on behalf of the client, there could be granularity and comparability altogether. Besides, cross-selling could be better managed/understood by the client. Similarly, by pooling advice from aggregators and financial institutions it will be fairly straightforward to distinguish between marketing and advice.
- Besides budget and human capital challenges for financial institutions, existing data governance frameworks might not be aligned to manage data quality in the big data context. Given the ubiquitous nature of data, it is a challenge for organizations to have a data governance framework that acknowledges the evolving definitions of data owners and consumers, addressing the risks related to the lifecycle of big data.

10. **Is the regulatory framework adequately addressing the risks mentioned above? Bearing in mind the constant evolution of technologies/IT developments and that some of the above mentioned regulatory requirements are not specific to the financial services sector (e.g. GDPR), do you think further regulation is needed to preserve the rights of consumers of financial services in a big data context? Please, explain why.**
    - It seems adequate. Further Regulation could bring new challenges that could erode the client's equilibrium. Risks related to data security or potential stealing, hacking or leaking of customer data are present in any company's day-to-day operations and, of course, also in the operations of financial institutions. For this reason, banks invest heavily in cybersecurity solutions and design every product, service and process having security in mind. We believe that the risks described above have existed since IT systems have been used for processing customer data. They will keep existing and are not specific of big data or of innovative uses of consumer data in the financial sector. There is no need to have specific regulation in this field for the financial sector.
    - In relation to the described risk regarding consumers having limited ability to challenge big data decision-making and seek clarifications, the GDPR reinforces the right to receive information about the logic and consequences for consumers of automated decision-making based on personal data. According to the GDPR, individual consumers have a right to explanation, human intervention and can challenge the decision. We consider that this mentioned risk is perfectly covered by horizontal regulation (i.e. GDPR) and there is no need for specific rules targeting the financial services industry. However, there is a need to clarify to what extent should explanations be given in order to strike the right balance with the needed protection of know-how, which must avoid full algorithm disclosure. Data protection authorities are the ones to clarify through the issuance of guidance.

11. **Do you agree that big data will have implications on the availability and affordability of financial products and services for some consumers? How**

could regulatory/supervisory authorities assist those consumers having difficulties to access financial services products?

- Yes. Identifying them and analysing how much of their credit risk is being subsidized, etc.

12. **Do you believe that big data processes may enable financial companies to predict more accurately (and act accordingly) the behaviour of consumers (e.g. predicting which consumers are more likely to shop around or to lodge a complaint or to accept claims settlements offers) and could therefore compromise the overarching obligations of financial institutions to treat their customers in a fair manner? Please explain your response.**
    - They can but, in any case, aggregators will prevent clients from unfair/biased treatments.
    - As for price adjustments based on consumer features and behaviour based factors, charging different prices to different individuals for the same product or service has been a common practice since old times. Pricing practices take different forms and evolve over time. Not always such pricing practices should be a concern, only when they are discriminatory with no objective foundation. Moreover, any assessment of pricing practices should be specific to the product and market in question. Furthermore, it is not the form of pricing what matters, but rather the effect on consumers or consumer outcome. The effect of such pricing depends on the market context. There is a need for an assessment on a case-by-case basis to avoid the risk of identifying the problem incorrectly and proposing an inadequate solution. Moreover, as a natural evolution of the use of consumer data by financial institutions, we expect prices to be driven down towards perfect competition, which will be a major improvement for consumers.

13. **Do you agree that big data increases the exposure of financial institutions to cyber risks? If yes, what type of measures has your institution adopted or is going to adopt to prevent such risks? What could supervisory/regulatory authorities do in this area?**
    - More than big data, it is the digitization of the industry what causes this increase of cyber risk.
    - We keep innovating in those areas in order to prevent/minimize even the most sophisticated attacks.

14. **Would you see merit in prohibiting the use of big data for certain types of financial products and/or services, or certain types of consumers, or any other circumstances?**
    - We do not agree. Asymmetries tend to be more difficult to fully understand and manage. Moreover, they tend to be a source of arbitrage.

15. **Do you agree that big data may reduce the capacity of consumers to compare between financial products/services? Please, explain your response.**
    - Disagree. It'll be better if accompanied by Aggregators.

16. **How do you believe that big data could impact the provision of advice to consumers of financial products? Please explain your response.**
    - People tend to be biased, while algorithms can avoid this. As a result, it should favor the discovery of new insights that can trigger well-motivated, more aseptic advice.

17. **How do you believe big data tools will impact the implementation of product governance requirements? Please explain your response.**
    - As in trading, algorithmic experts will have to take large responsibility on the intelligence being deployed in production.

18. **How do you believe big data tools will impact know-your-customer processes? Please explain your response.**
    - It should make it easier and more robust, as it can get information directly from different data sources to enhance the onboarding process or check beyond the standard process. Outliers can easily be marked for an ongoing track.

POSSIBLE EVOLUTION OF THE MARKET

19. **What are key success factors for a big data strategy (i.e. the adaptation of the business model/plan towards big data driven technologies and methods)?**
    - Fair impact measurement: key to internally prove value of big data without under- nor overselling its added value.
    - Techniques against overfitting of the parameters: typically, data-driven processes generate models too tightly linked to the database.
    - An effective big data strategy should be a highly dynamic roadmap for the future and a work in progress to be adapted. It is a continuous journey characterized by change and flux. Business adoption of big data requires addressing issues of organizational alignment, business process design, coordination and communication.

20. **What are the greatest future challenges in the development and implementation of big data strategies?**
    - Senior management with critical judgement on the overlap: technology, science and risk management (not only valuation of the risks but, more relevant, their hedging, etc.).
    - Avoid internal overbuying of the big data approaches: as the whole industry and regulation sharply move towards big data strategies, the management of the different units that first avoided digitization could rapidly change attitude and embrace inorganic change. Big data managers need to control this change to avoid deceptions - big data is a tool, not a solution in itself.

21. **This Discussion Paper refers to a number of measures and tools meant to ensure compliance with conduct and organisational regulatory requirements as well as data and consumer protection rules in the context of big data analytics. Are other measures and tools needed? If so, what are they and what they should cover?**

22. **How do you see the development of artificial intelligence or blockchain technology in connection with big data processes?**
    - AI within big data is simply a natural step. They will keep evolving hand-in-hand.
    - When it comes to big data and AI, we are at the early stages, at the emergence of what the potential value of convergence can be. As AI progresses and evolves, some of the basic tasks that data scientists perform routinely, might be automated and will yield productivity (automating the more basic tasks and reserving the more complex ones for data scientists).
    - The connection between big data and blockchain will come from the development of a new field of analysis: the application of big data techniques to the information stored in distributed ledgers. The implementation of blockchains will allow to have shared detailed transactional and personal data which open new possibilities of pattern analysis about, for example, customers spending habits. And, when introducing smart contracts, they can be analysed as future liabilities that can be used for risk scoring management. Thus, more advanced AI technologies will allow a more precise prediction of future economic needs and behaviors of customers through smart contracts portfolio analysis .

ADDITIONAL COMMENTS

23. Are there any other comments you would like to convey on the topic of the use of big data by financial institutions? In particular, are there other relevant issues that are not covered by this Discussion Paper?