Data protection, fairness and sharing

Sébastien Raspiller

Assistant Secretary, Ministry of Economy and Finance, France

Financial services and data: a regulator's perspective

The decision adopted in early February by the Bundeskartellamt to limit data pooling practices, which means combining user data from different sources, by Facebook without the user's consent is the first decision made by a national authority combining data protection and competition regulation. This decision certainly emphasizes the need for the public authorities to take into account the evolutions of the market practices of dominant actors of the digital economy regarding competition law. The situation may be somehow different in the financial sector, given the diversity of its actors, although competition matters, precisely for this reason.

What are the main opportunities to further leverage data from both customer's and financial institutions' points of views?

It is commonly admitted that data is the 21st century's oil and the main resource in a digital based economy. This is true as well for the financial services, which will certainly undergo major transformations.

As the digital shift is fueled by data, it is of paramount importance for the financial services providers to secure the access to both customers' personal data and general data. From a commercial standpoint, the use of data can serve as a catalyst for the development of new business models and new products and enhance the delivery of financial services to customers. For instance it may help develop insurance solutions targeted for SMEs. The financial institutions' internal management is also expected to be disrupted with the use of data and data analytics in a wide range of applications such as the fight against fraud in the financial sector or the implementation of the anti-money laundering regulations. From the customer's perspective, the benefits expected from a growing data based financial services offering are a higher diversity associated to a greater individualization of services, enhancing satisfaction.

How is data sharing impacting innovation opportunities?

In a growingly digitalized economy, the special features of data as intangible and highly mobile resources make data sharing an important stake for the emergence of innovative actors and new markets. In the financial sector, data sharing refers to the process of making data available to the consumer itself (portability) but also multiple third parties (interoperability) in order to offer a wider range of products and services.

>>>

>>> By making easier for financial institution to access new and reliable information, data sharing fosters innovation and new areas of competition.

It is the role of public authorities to encourage financial institutions to develop data sharing strategies and interoperability in order to spur innovation and new business models. Regulatory initiatives have already be taken at the EU level such as the facilitated use of API to ease interoperability of data within the implementation of the PSD2 framework, or the right to data portability created by the General Data Protection Regulation (GDPR) which allows individuals to obtain and reuse their personal data for their own purposes across different services. Moreover, actions could be taken to foster the use of distributed ledger technologies as relevant tools to data sharing models.

What are the main risks data face and related consequences?

The emergence of data as key resources for the digital economy and financial institutions has at the same time contributed to expose these actors to a whole new set of risks. Even if firms have been exposed to cyber risks and cyber-attacks for a couple of decades, the growing part of data in these companies' value and business renew the approach of managing such risks.

First, financial institutions are faced with common cyber risks, which can either be malicious or accidental, such as a destruction or corruption of data bases, leaks of confidential information or thefts of intellectual property. Second, the loss of reputation due to data leaks or public revelations of prohibited uses of data are increasingly growing risks. Third, regulatory requirements and compliance to data protection regulations constitutes a major risk that should be taken into account in the data managing strategies as regards the powers now held by supervisory authorities. ●

Leena Mörttinen

General Director, Financial Markets Department,
Ministry of Finance, Finland

New realities of the information economy

The honeymoon with the information platform economy is over. The pendulum swinging back from the state of naïvely sharing data with everybody to a state of uneasy paranoia of who is manipulating us. The "surveillance capitalism" is now a suspect in providing means to hostile players to use our data against us and our societies.

How can we ensure that our identities and societies are kept safe? Financial services are a good reflection point for this debate. After all, my bank knows everything about me. There are important boundaries that deserve attention. These lie between the big tech companies, banks, the individual and the state.

The first conflict is the growing competition on data. Both banks and big tech need this resource. However, banks are in the business of trust. Unlike a social media platform, they cannot sell our innermost thoughts to political consulting firms.

Creating a level playing field between banks and big tech is a huge challenge. In the financial sec-tor, we are used to regulating balance sheets, not data and its use. This is about to change as we move from regulating entities to regulating activities. As lawmakers, we will pay more attention to effective consumer protection. However, we need a better understanding of the challenges particular to quickly evolving >>>

>>> platform business models and technological advances. The EU General Data Protection Regulation is a first step and it affects banks and big tech alike.

The second difficult boundary lies between the business and the state. Financial infrastructure is critical for the stability of any society. After the last financial crisis, we have improved the capabilities of both companies and authorities to withstand economic shocks. We also need to ensure that we are equally well prepared to systemic risks stemming from severe operational incidents. We trust cashless payment services to be available 24/7. If the flow of money were to stop due to a major cyber-attack, panic would ensue within hours. The aim of the EU financial services legislation is a fully integrated financial system. Irrespective of this, every member state should be able to ensure the continuation of critical services depending on the threats that are particular to its geography.

Finally, we have to redefine the boundary between the individual and the state. Also here banks have become the pressure point. With an increasing concern of money laundering, banks will face new and tougher regulation and supervision to ensure that the critical infrastructure is not used for illegal purposes.

However, with tougher supervision, authorities need to think carefully how to ensure the individual's fundamental right for privacy. Bank account information shows who we really are. When should the authorities be allowed to use it? Our liberal western values do not go well with continuous state surveillance of citizens. We should be careful that we do not end up falling into this model without careful ethical consideration.

Money is data and it must be kept safe and flowing while preventing the destabilizing use of our infrastructure against us. We need a new regulatory framework and deep ethical discussions to be able to find answers to the questions posed by the new realities of the information economy. Security will come at a high cost. The only way to make this worth the while of our financial institutions is a deeply integrated banking union and a well-functioning capital markets union that pro-vide the scale economy benefits. If we do not succeed in this, we will likely remain a data colony with mainly imported services, and if we are not careful, with imported values as well. ●

Joe Cassidy

Partner, KPMG

The future of data ethics and the value of trust

Data analytics, including intelligent and autonomous systems, have become part of our everyday lives – and ubiquitous in all sectors, including financial services. However, if these increasingly public-facing and high-profile systems are to continue to serve the public interest, and deliver fair and transparent outcomes, we need ethical principles, policies and guidelines to govern their development.

Recent regulation of data protection (i.e. GDPR) and privacy constitutes a good start, but a holistic view of data ethics covers more than just compliance. It should encompass the growing volumes of customer data, access to and storage of data, and data flows (often across national borders) between financial institutions and third-party service providers.

The increased use of the spectrum of intelligent and autonomous systems (including Machine Learning, and the use of Artificial Intelligence), to automate decision making on customers is clearly an area policymakers are rightly concerned about. The results of these decisions can be life changing for customers – in areas of life insurance, finance, healthcare access and even travel. Consumers are also likely to become increasingly aware of the value of their data, and of the ways in which it is being used, leading to denial of access issues and possibly data manipulation by consumers.

Intelligent and autonomous systems requiring little or no human intervention can greatly boost the efficiency and effectiveness of organisations, for example by improving fraud detection and supporting cost reduction. But while such systems help the organisations to 'work smarter', they might not automatically optimise fair outcomes. For >>>

>>> example, where the 'black box' is designed to lead consumers towards pre-specified outcomes that benefit the provider rather than the customer, and where similar strategies based on similar data sets lead to herding behaviour or ignore situations that are not captured in the data.

Organisations may struggle to identify the limitations of these systems at an early stage, and to ensure their outputs are free from prejudice, whether conscious or unconscious. However, core principles should include respecting an individual's ability to make their own free choice; operating with transparency and delivering data outcomes within the boundaries of a glass box; and installing an organisation-wide approach to data ethics together with clear principles of accountability – in order to demonstrate a robust governance framework that places the ethical use of data at the top of the agenda.

"A holistic view of data ethics covers more than just compliance."

- JOE CASSIDY

It's logical that the use of personal customer data combined with the autonomous, ML and AI systems must be subject to challenge and be open to legal and regulatory scrutiny in order to establish much higher ethical standards. This is a very significant debate and for data analytics to be a force for good it will require a co-ordinated effort from both industry and regulators.

Now is the time for all stakeholders to build on existing international and cross-sector work, focusing in more depth on the specific customer impact risks and challenges. Rather than create an entirely new set of ethical principles, our aim is to move the debate forward with foundational actions. ●

Nina Arquint

Head Group Qualitative Risk Management, Swiss Re Management Ltd.

A multi-faceted approach needed to address data challenges

We are in midst of a "data revolution" of our society and our economy. To harness the full innovative potential that big data and AI provide, financial service providers must ensure that consumers trust them to handle their data transparently and fairly. While studies show that financial institutions currently enjoy higher levels of consumer trust than other users of data, this trust must be safeguarded by continued responsible business conduct. At the same time, financial institutions, and insurers in particular face multiple challenges with regards to using data in a way which is in the customers' best interest.

Fairness in utilising data is at the heart of what insurance has done for so many years. Insurance is first and foremost transforming data into an assessment of riskiness. It means fixing the price at which individuals can enter a pool of insured, and can benefit from the protection that the insurer generates for its pool members. To be able to facilitate a fair risk assessment, the insurer needs access and permission to use the data of those that need the protection of the pool. As more restrictions are applied to the use of data for setting premiums, the risk of adverse selection increases which undermines the concept of insurance. All this raises legitimate questions about solidarity and fairness in insurance. This is a necessary and unavoidable discourse, which at the end of the day is one about values. Societies must inevitably decide to what extent solidarity should be enforced.

The frequency and severity of ethical issues has increased over the past few years indicating the need for companies to address their digital responsibilities. Ethics is not a universal concept, and values may often be in competition with each other. The firms have a clear reputational incentive to address these ethical issues, and to be transparent about this. Regulators should monitor this process and, where necessary ensure that good industry practice is adhered to.

Outsourcing and the ability to share data across borders enables customers to access innovative services in many areas. New, often fragmented regulatory requirements that limit cross-border data sharing or restrict outsourcing could hinder the industry in the development of a compelling digital service portfolio. Insurers are not only subject to the harmonized European Data Protection Regulation, but are additionally being examined by insurance supervisors on how they use (big) data.

"Data challenges are best addressed in close collaboration between the industry and regulators."

- NINA ARQUINT

Regulators must find the right balance between protecting consumers, while not standing in the way of innovation to the benefit of consumers. In doing so, they have the chance to support firms in dealing with the challenges mentioned above. Instead of placing restrictions on cross-border data sharing, regulators can play a role in supporting the development of internationally harmonized data protection rules. Regarding outsourcing and cloud use, regulators should ensure that insurers have processes in place to identify, manage and mitigate relevant risks. By all means, regulators should not impose excessive requirements or outright bans which would subject insurers to unreasonably higher standards than others. Finally, regulators must also acknowledge that some of these challenges cannot be addressed via the regulatory process alone. ●

Simona Șandru

Head of Complaints' Department, National Supervisory Authority for Personal Data Processing, Romania

Data protection - a good economic "asset"

The protection of personal data has become during the last two decades one of the most important issues to have in mind in the business environment, whenever this kind of information is considered to be an added value for the success on the market.

Taking into account the present globalized and technologically-driven economic relationships where intrusions into private life are most likely to occur without the knowledge of the concerned individuals their legal protection has to be a cornerstone for any rule-of-law government.

"We think that responsible implementation of the GDPR by all players involved will achieve both its objectives: defending the individuals' fundamental rights and functioning of the internal market."

- SIMONA ȘANDRU

In this regard, the European Union (EU) adopted numerous pieces of legislation aiming at ensuring a high level protection of personal data processed by every single actor involved in professional or commercial activity: natural persons, micro, small and medium-sized enterprises, large companies, groups of undertakings, public bodies, and other types of organisations ("data controllers" or"data processors", as the case may be). The exceptions from the established legal framework are just a few and require a strict and limited interpretation and application.

The Regulation (EU) 2016/679 (the General Data Protection Regulation, known as "GDPR"), which entered into force in 2016 and is fully applicable in all Member States as of the 25th of May 2018, but also the Convention 108/1981, modernised by the Council of Europe in 2018, set an even higher level of protection requirements for the EU residents' personal data. These legal instruments tend to impose the European good model of human rights' protection as an international standard model for data protection.

For this model to work, it is essential to have some mechanisms of control put in place; this role is undertaken by the independent supervisory authorities established in every Member State (and also at EU level), which are equipped with equivalent investigative, corrective, authorisation and advisory competencies. In order to ensure a coherent and consistent approach across the EU, some legal issues, especially those related to the cross-border processing operations, shall be dealt with by a newly set up body, the European Data Protection Board (EDPB), composed of representatives of all EU supervisory authorities.

The EDPB's vivant activity is already available for all the interested parties, whether controllers or individuals, in the issued papers aiming at ensuring a proper and detailed explanation of different notions of the GDPR (such as consent or transparency). Additionally, the EDPB has developed guidelines in order to help organisations in adopting binding corporate rules and codes of conduct or adhering to certification mechanisms. These tools have been introduced by the GDPR as alternative safeguards for the protection of personal data, as regards the transfers from the EU to third countries and international organisations, and also in other contexts, regarding the implementation of security policies, for instance. ●

Konstantinos Botopoulos

Advisor to the Governor, DPO, Bank of Greece

Data challenges for central banks

With the advent of the GDPR, the new "Constitution" in the field of data protection, another landscape has emerged. Although the modifications vis-à-vis the old regime and the new provisions are not all revolutionary per se, the effort required by those competent for the protection stemming from the GDPR has changed both in scale and quality.

The name of the game is now "self-regulation" but also "holistic protection". The public authorities have less scope for intervention, which has been taken up by the newly established DPOs (Data protection Officers). The role of the latter is global and central: although DPOs are not to be held responsible for any omissions or problems occurring under their watch, they are responsible, in the practical sense, of the necessary arrangements, most notably of technological nature, the cooperation within institutions and with the competent authorities and the overall "ticking of the system".

Such system, complex and demanding by nature, constitutes a world of its own in the case of big institutions, such as banks and even more Central Banks. The quantity and sensibility of data, the juxtaposition of competences, the numerous contacts with outsiders, the intra-European nexus, and the quasi-systemic importance of preventing leaks –all those elements require not only a concentrated effort but a considerable change of culture. Within Central Banks, and around the DPO, the most common form of organization consists of a DPO-office, for which should be chosen persons with administrative, legal, IT and risk-management capabilities, and a cycle of representatives of the various departments of the Bank, providing the necessary connection with the practitioners dealing with data.

At the Bank of Greece, we have also established a Steering Committee comprised of the Heads of the departments most involved and discussing strategic directions and challenges. Cooperation and collaboration are of the essence, as well as the creation of a collective conscience within the >>>

>>> Bank that data protection is a must both from a legal and a reputational point-of-view.

The next level, the European harmonization of practices, is being put into place through the European Authority which has been created by the GDPR and, especially for Central Banks, through expert groups meeting regularly. It is still too early to judge the effectiveness of such forums and the overall impact of the GDPR in the central banking sector. It could provide an occasion, however, for enhancing the technological capabilities of the Banks, getting rid of unnecessary data, promote a more open relationship with citizens and advance European banking integration. Only thus would the effort, the cost and the administrative burden imposed by the GDPR be justified and fructified. ●

Patricia Plas

Head of Public Affairs, AXA Group

GDPR: one year after its implementation

2018 marked the beginning of data privacy awareness initiatives all over the world. A recent survey reveals 66% of the French population affirms being more conscious of data protection than before and about the same percentage now say they have heard about General Data Protection Regulation (GDPR). This is substantial.

How is this framework perceived? The results are positive overall even if we are still in its early stages. Consumers' awareness of their rights regarding the protection of their data has increased the community's vigilance. The European data protection authorities have all seen the number of complaints and sanctions increase: 317 complaints were filed with the Belgium APD in the first 6 months of GDPR compared to 13 in 2017; over 10,000 data breaches were reported to the Dutch, German and British authorities. These provide an opportunity for the entities involved to rethink their organization. The first GDPR sanction was initiated by the French CNIL resulting in Google being fined €50 million in January. In addition, the European Data Protection Board has been active in briefing organizations, like SMEs, on their obligations under the GDPR. Throughout Europe, there is a clear-cut "pre" and "post" GDPR era; history will refer to GDPR as the turning point where privacy became tangible.

As European companies have no choice but to invest heavily in protecting all the personal data they handle while companies in other countries experience less constraints, some do see GDPR as a competitivity blocker first. Yet, GDPR's growing successes are raising data privacy's appeal in other jurisdictions, notably because GDPR has an extra-territorial scope allowing it to protect EU residents regardless of where the data processing occurs or how cross-border data flows are arranged.

"The question of data protection is gaining ground in other jurisdictions."

- PATRICIA PLAS

Although such legal rigor on the handling of personal data exists in practice only in Europe, the question of data protection fueled by GDPR's release in great pomp, is gaining ground in other jurisdictions. This may reflect a global shift towards greater privacy protection under the emergence of a caring coherent approach to the free movement of data in the EU and possibly beyond.

In January, the Commission adopted its adequacy decision allowing for the free flow of personal data between the EU and Japan creating "the world's largest area of safe data flows". China itself is in the early stages of creating a data protection regulatory system to police Chinese social networks in response to consumer pressure. The United States have started discussing data privacy at the federal level, a conversation that would not have come about without GDPR, which directly inspired a privacy law passed in California in 2018.

What remains to be seen is at what pace and to what extent any genuine convergence can be achieved as diverging strategies in AI could for instance also impact its evolution. Meanwhile the EU, as in other policy areas, is sending a clear message: getting access to the fast-growing EU data economy - €739 billion by 2020 likely to be boosted by the recent regulation on the free flow of non-personal data - means complying to the highest-privacy standards. ●