BBVA | Research

Digital Economy Outlook

April 2017 | DIGITAL REGULATION UNIT

BBVA | Research

Index

Closing date: 15 April 2017

1. Summary

Digital platforms: economic features and policy challenges. Digital platforms have already transformed a broad range of industries (content, transport, accommodation and retail shopping) and they will continue to do so with other sectors. This article provides an overview of the economic features of these platforms and identifies some general challenges for public policy.

Fostering a data-driven economy in the EU: an adequate regulatory framework to encourage data-driven services. The European Commission (EC) intends to foster an efficient competitive single market for data services like cloud computing, among others. To achieve its goal, it needs to identify legal, economic and regulatory challenges. It will enter into a dialogue with cross-sector stakeholders to find out about barriers and current industry practices. Before reaching conclusions, the EC plans to go through a phase of experimentation and testing.

Licensing Fintech companies. Authorities are trying to strike a balance between fostering innovation and ensuring financial stability. The beginning of the year is marked in the USA by a sports event that catches the attention of most Americans, the Super Bowl. However, this year, a square-off among American Financial Supervisors tried in vain to steal the limelight.

Behavioural biometrics, a step further in digital identification for financial services. As the world becomes more digital, financial institutions need to keep up with consumer demands. The use of biometrics in the banking industry has been gaining traction thanks to the arrival of devices that already include biometric readers and the expansion of wearable banking. The increasing scale and frequency of cyber attacks against user accounts in the past few years has shown that security cannot rely on identification means based solely on static biometric elements that can be compromised. Behavioural biometrics could be a solution to combating fraud and identity theft**.**

The governance of technology in the digital world. Some emerging technologies follow an exponential growth and adoption rate, and adopting them demands governance adapted to complexity and rapid change. In the case of the Internet, the model based on a combination of international cooperation and collective participation has so far – despite the internal debates– responded to the most significant challenges and may therefore serve a benchmark for governing other exponential technologies.

2. Digital platforms

Economic features and policy challenges

Digital platforms have already transformed a broad range of industries (content, transport, accommodation and retail shopping) and they will continue to do so with other sectors. This article provides an overview of the economic features of these platforms and identifies some general challenges for public policy.

Intermediaries in multi-sided markets

From an economic point of view, digital platforms act as intermediaries in two- or multi-sided markets. These are markets in which two or more different groups of agents (e.g. buyers and sellers) obtain value from becoming connected or coordinated in some fashion, but transaction costs (search, bargaining, enforcement, etc.) prevent these agents from solving that externality directly. Platforms are able to internalise the externalities by minimising transaction costs and facilitating direct interactions between the different sides of the market (Evans and Schmalensee, 2007)[1]. As well as these matching benefits, some types of platforms bring other benefits, for instance "discovery benefits" in the case of content distribution platforms (e.g. Spotify) or a more intensive use of physical assets in the case of sharing economy platforms such as Airbnb (Coyle, 2016)[2].

Some traditional businesses can be characterised as platforms operating in two-sided markets. For instance, traditional bazaars, which connect retailers with customers; newspapers, with readers on one side and advertisers on the other; or auction houses, which bring together buyers and sellers of art and collectibles. In recent years, new types of digital platforms have emerged and multi-sided markets are experiencing a great surge. This has to do with the opportunities that information and communication technologies have created to significantly reduce transaction costs and facilitate direct interactions between individual agents. In this regard, Coyle (2016) argues that platforms achieve improved economic coordination through the use of technology, since participants do not need to be co-located or to transact at the same time.

Different classifications of platforms have been proposed. Some of them are based on the type of agents that form each side of the market, such as the distinction between business-to-business (B2B), business-to-consumers (B2C) and peer-to-peer (P2P) platforms. Other classifications focus on the role performed by the platform. For instance, Evans (2003) proposes three broad categories of platforms[3]:

- **Market makers**: they enable the different groups of agents to transact with each other (e.g. online marketplaces or shopping malls).

1: Evans, D., & Schmalensee, R. (2007). The Industrial Organization of Markets with Two-Sided Platforms. *CPI Journal*, 3.
2: Coyle, D. (2016). Making the most of platforms: a policy research agenda. Jean-Jacques Laffont Digital Chair.
3: Evans, D. S. (2003). Some empirical aspects of multi-sided platform industries. *Review of Network Economics*, 2(3).

- **Audience makers**: they match advertisers with audiences (e.g. traditional mass media, Internet portals or social networks).
- **Demand coordinators**: they develop goods and services through coordination (e.g. software platforms or payment systems).

Indirect network effects

As appears from the definition of multi-sided markets, one of the most significant characteristics of platforms is the presence of indirect network effects. A good exhibits an indirect network effect if its demand depends on the provision of a complementary good, which in turn depends on demand for the original good (Rysman, 2009)[4]. In the case of platforms, think of the complementary good as being the contribution of the other group of participating agents. This means that the utility of consumers on one side of the market increases with the number of consumers on the other side. This effect has significant implications for both business strategies and the structure of multi-sided markets.

For entrant platforms, indirect network effects raise the chicken-and-egg problem. Platforms need to get both sides of the market on board to trigger a positive feedback loop that makes the market grow. In order to do so, they may follow different strategies: offering low prices or even transfers to one side of the market, investing in lowering the participation costs of one group of customers, or initially directly supplying one side of the market (Evans, 2003).

Mature platforms still have to set pricing structures that take into account indirect network effects. Indeed, Rochet and Tirole made the pricing structure central to the definition of multi-sided markets. “A market is two-sided if the platform can affect the volume of transactions by charging more to one side of the market and reducing the price paid by the other side by an equal amount”, they wrote in their 2006 paper[5]. Therefore, optimal prices depend not only on marginal costs but also on the price elasticity of demand on each side and the nature and intensity of indirect network effects (Evans and Schmalensee, 2007). In practice, participants on one side of the market tend to subsidise these on the other, depending on the nature and intensity of indirect network effects and the extent of “multi-homing” on each side (Evans, 2003; Armstrong, 2006)[6].

Moreover, to keep both sides of the market on board, consumers need to have confidence to interact or transact with those on the other side. Thus, platforms generally employ different techniques to mitigate information asymmetries, reduce risks and build trust between the participants. They provide rules on access and participation, sanctions against misbehaving agents, standard contracts, rating and review systems or escrow payments (Coyle, 2016). In this regard, since platforms have incentives to devise rules that promote positive externalities between customers and limit the negative ones, some authors argue that they serve as rule-making governance institutions (Boudreau and Hagiu, 2007)[7].

4: Rysman, M. (2009). The economics of two-sided markets. *The Journal of Economic Perspectives*, 23(3), 125-143.
5: Rochet, J. C., & Tirole, J. (2006). Two-sided markets: a progress report. *The RAND journal of economics*, 37(3), 645-667.
6: Armstrong, M. (2006). Competition in two-sided markets. *The RAND Journal of Economics*, 37(3), 668-691.
7: Boudreau, K. J., & Hagiu, A. Platform Rules: Multi-Sided Platforms As Regulator. In *Platforms, Markets and Innovation*, edited by Annabelle Gawer. Cheltenham, UK: Edward Elgar Publishing, 2009.

Indirect network effects also impact the structure of multi-sided markets. In general, it is argued that they promote larger and fewer platforms, i.e. market concentration (Evans and Schmalensee, 2007; Gürkaynak et al., 2016)[8]. The chicken-and-egg problem generally makes barriers to entry higher and, for successful platforms, the self-reinforcing feedback loops between both sides of the market can trigger the threat of tipping (Bundeskartellamt, 2016)[9]. However, since incumbent platforms might also quickly lose their market share due to negative feedback loops, the role of indirect network effects can be to some extent ambivalent.

Besides indirect network effects, other factors affect the structure of multi-sided markets. On the one hand, economies of scale and direct network effects can reinforce the trend to concentration. Platforms usually benefit from economies of scale since their intermediation activities involve significant fixed costs. Direct network effects are present in some platforms (e.g. social networks) since consumers on one side of the market directly value the number of peers. This increases consumers' cost of switching between competing platforms and, therefore, raises barriers to entry. On the other hand, there may be counterbalancing factors against market concentration. These are differentiation between platforms (vertical or horizontal), "multi-homing" — which usually results from horizontal differentiation — and platform congestion — not relevant in the case of digital platforms — (Evans and Schmalensee, 2007). These are similar to the factors identified by Rysman (2009) as determining whether "tipping" towards a "winner-takes-all" situation occurs.

Challenges for public policy

Digital platforms create economic value and can therefore benefit all agents involved. However, since they reconfigure how economic activities take place — moving from one- to multi-sided markets —, they give rise to new risks and concerns that policymakers must address. These are some of the most significant ones:

- **Level playing field**. Some platforms might take advantage of regulatory loopholes to provide services subject to lighter requirements than those imposed on one-sided markets. To avoid these situations, the regulatory framework needs to evolve to ensure that similar activities receive similar legal treatment.

- **Consumer protection**. In multi-sided markets, consumers interact with both the platform itself and the other sides of the market. The degree of intermediation — and thus the extent of direct interaction between the agents — depend on specific business models. To ensure consumer protection is not weakened in such a framework, there is a need for clear and transparent assignment of responsibilities.

- **Negative externalities**. The activity of some platforms may have negative effects on agents that do not participate in those markets. For instance, the increase of short-term visitors in residential neighbourhoods or the potential implications for the financial system of lending marketplaces. Public policies need to mitigate these negative externalities.

8: Gürkaynak, G., İnanılır, Ö., Diniz, S., & Yaşar, A. G. (2016). Multisided markets and the challenge of incorporating multisided considerations into competition law analysis. *Journal of Antitrust Enforcement*, 0, 1-30.
9: Bundeskartellamt (2016). *The Market Power of Platforms and Networks*, Working Paper B6-113/15.

- **Promote competition**. Data plays a key role in many digital platforms and might restrict competition if it raises significant entry barriers and/or switching costs. In this regard, regulations that allow consumers to securely transfer their data between different firms can promote competition.

- **New tools for antitrust analysis**. Conventional methods to define the relevant product market or to measure market power are generally not applicable (at least straightforwardly) to multi-sided markets. For instance, the marginal-cost pricing is not a relevant benchmark, given the optimal pricing structure of platforms. Besides, network effects are usually relevant to assess potential anticompetitive practices.

- **Impact on other public policies**. Due to their intermediation role, platforms can help governments to collect certain taxes. Moreover, “gig work” platforms have significant implications for labour and social protection policies that governments need to analyse and take into account.

3. Fostering a data-driven economy in the EU

An adequate regulatory framework to encourage data-driven services

The European Commission (EC) intends to foster an efficient competitive single market for data services like cloud computing, among others. To achieve its goal, it needs to identify legal, economic and regulatory challenges. It will enter into a dialogue with cross-sector stakeholders to find out about barriers and current industry practices. Before reaching conclusions, the EC plans to go through a phase of experimentation and testing.

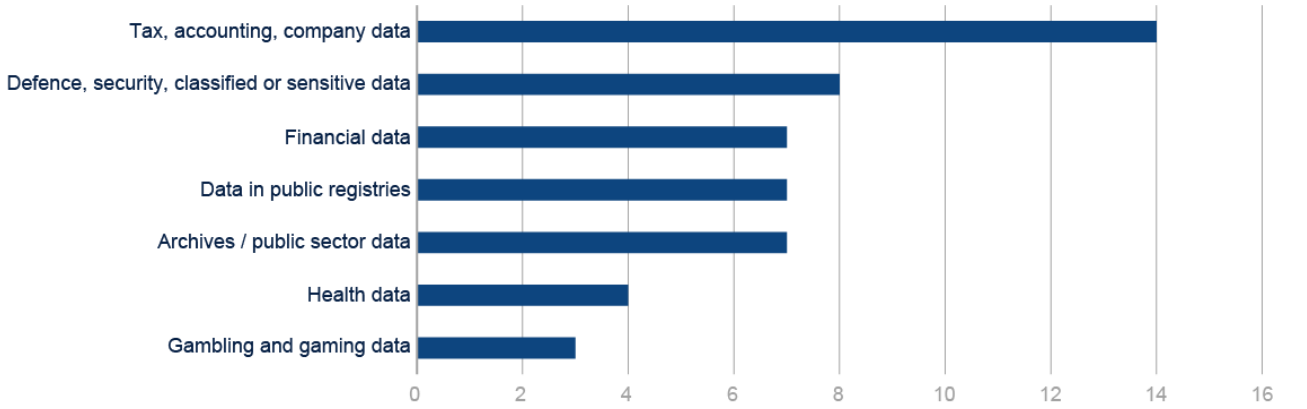
Free flow of data and localisation restrictions

Data localisation restrictions derive from national legislation or administrative disposals, guidelines or practices that constrain, either directly or indirectly, localisation of data for its storage or processing. Restrictions for reasons of personal data protection are already covered in the General Data Protection Regulation (GDPR). However, the EC plans to tackle obstacles impeding the free flow of data within EU borders for other reasons beyond the protection of personal data. Removing existing data localisation measures would lead to GDP gains of up to €8bn a year[10].

Some legal provisions of EU Member States include localisation of invoices, books and records and accounting documents to stay on the premises of the company or on servers within the country. Sector specific restrictions include health, gaming and gambling or financial data. Not only privately held data are affected by restrictions but also public sector data. For instance, in France there is a prohibition for local authorities to use cloud computing services without a special certification for storing and processing any document received by public authorities. According to the analysis performed so far by the EC[11], in a sample of 50 restrictive measures identified in 21 Member States, the highest share of data localisation restrictions applies across sectors and, in many cases, to privately held data. Moreover, it is not only a matter of restrictive rules but also of perception. In this respect, a recent study outlined that "perceptions are as powerful as hard restrictions in deterring cross-border data transfers"[12]. Policy initiatives aimed at promoting existing relevant certifications and standards and at removing data localisation restrictions would increase benefits for users and providers of cloud computing, as well as for society as a whole to a total of over €19bn between 2015 and 2020[13].

10: *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE, 2014.
11: *EC Staff Working Document accompanying the EC Communication on Building a European Data Economy*, January, 2017.
12: *Facilitating cross border data flow in the Digital Single Market*, London Economics, 2016.
13: *Measuring the economic impact of cloud computing in Europe*, Deloitte, 2016.

Figure 3.1 Data localisation measures per sector/type of data



Source: Staff working document on the Free Flow of Data and emerging issues of the European data economy, accompanying the Communication on Building a European Data Economy, January 2017

Access and re-use of non-personal machine-generated data

In the IoT (Internet of Things) or smart devices context, non-personal machine generated data do not have a specific regulatory framework, as regards their access, transfer and re-use. There is no clear framework either for interoperability, portability or standards in relation to non-personal machine-generated data. The EC is currently analysing the extent to which this type of data are exchanged and traded and whether there is a need for any regulatory or EU policy initiative to foster access and re-use of this type of data and incentivise the sharing of such data. As for the possibilities for addressing the issue, the EC is considering the following: a) guidance on incentivising businesses to share data; b) fostering the development of technical solutions for reliable identification and exchange of data; c) default contract rules; d) access for public interest and scientific purposes; e) data producer's rights; f) access against remuneration.

A number of companies are opening up some of the data they hold through Application Programming Interfaces (APIs) for access by third party applications. However, making data available to third parties remains uncommon. Data sharing can take a number of forms: merger & acquisition and venture capital investment, joint ventures, data trading among independent economic operators, the usage of data innovation spaces or adding data gathering and analysis to traditional services and products. However, data trading among independent economic operators accounts for a very low number of companies[14].

As a comprehensive policy framework does not exist, the solution in the meantime is largely left to contractual agreements. The most common issues occurring in complex data clauses are: the possibility for a party to re-use or communicate data to third parties; ownership of data generated or processed; allocation of any IP rights at stake

14: "Impact assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data and liability (Deloitte, first interim report forthcoming)", on *EC Staff working document accompanying the EC Communication on Building a European Data Economy,* January 2017.

generated by technical devices; and the extent to which parties who have access to data are allowed to commercialise it[15]. Sector-specific legislation regulates access to privately-held non-personal or anonymised data in certain contexts. For instance, access to in-vehicle data for the purpose of opening up the market for after-sales services like maintenance and repair is subject to a regulated regime. Also, the PSD2 (new Payments Services Directive) opens up payment information under certain conditions, affecting both personal and non-personal data.

Liability, interoperability, portability and standards

As for data products based on IoT (Internet of Things) or AI (Artificial Intelligence), highly complex interdependencies which are being formed between their different layers are significant elements of their operation. When damages occur in the context of the use of such technologies, legal challenges arise in relation to liability assignment, as well as regarding product compliance, safety and insurance-related aspects. Liability in relation to IoT products and services has been identified as a specific issue to be tackled as part of the Digital Single Market Strategy. The EC has invited stakeholders to explore the feasibility of other approaches that may provide interesting avenues for addressing this challenge. Discussions revolve around the following options: a) strict liability regime; b) risk-generating approach; c) risk-management approach; d) voluntary or mandatory insurance schemes.

Portability is understood as the ability to move, copy or transfer data. The GDPR introduces a portability right in the context of personal data, so that data subjects can benefit under certain circumstances and download their data or have their data directly transmitted to another service provider. However, uncertainty remains as regards portability in a non-personal machine-generated data context. Data portability considerations are closely related to questions of data interoperability, which enables multiple digital services to exchange data seamlessly, facilitated by appropriate technical specifications and standards. According to the EC, there are several possible ways to tackle this issue: a) developing recommended contract terms to facilitate switching of service providers; b) developing further rights to data portability; c) sector-specific experiments on standards.

Conclusion

Data has become the new oil of the twenty-first century and the EC is aware of it. European authorities are now analysing and engaging in a dialogue with the industry and other stakeholders to foster data-driven services and the free flow of data within EU borders. Data localisation restrictions for other reasons apart from the protection of personal data, access and re-use of non-personal machine generated data, liability, interoperability and standards in this context are among the issues to be tackled by the EC in its Free Data Flow Initiative. The EC is aware that before reaching conclusions, there is a need to test these issues in a real-life environment in partnership with stakeholders.

15: Legal study on ownership and access to data, Osborne Clarke for the European Commission, 2016.

4. Licensing Fintech companies

Authorities are trying to strike a balance between fostering innovation and ensuring financial stability

The US debate

The beginning of the year is marked in the USA by a sports event that catches the attention of most Americans, the Super Bowl. However, this year, a square-off among American Financial Supervisors tried in vain to steal the limelight.

This unusual confrontation started in December 2016, when the US Office of the Comptroller of the Currency (OCC), one of the main US Financial Supervisors, issued a whitepaper outlining its intention to grant special purpose national bank charters to Fintech companies.

State financial authorities led by the New York State Department of Financial Services Superintendent (NYDFS) reacted immediately, opposing this announcement by claiming that it didn't fall under OCC competences. Critics also highlighted the potential negative impact of this charter on financial stability and consumer protection. Despite Republican and Democratic representatives joining the defense team, the OCC has continued to gain yards, finally issuing a Draft Licensing Manual Supplement for Evaluating Charter[16].

Although this conflict illustrates the global debate on the best regulatory strategy towards Fintech, the OCC's rather restrictive approach seems to have disregarded the steps taken by other countries on this topic.

Is there a case for granting Fintech companies special purpose licenses?

Before answering this question, we should establish what is understood by a 'Fintech company'. According to the European Parliament draft report on Fintech[17], "FinTech may be understood as finance enabled by new technologies, covering the whole range of financial services, products and infrastructure". However, it appears that discussion currently focuses on non-banking companies providing services that are subject to oversight by Financial Authorities when offered by financial institutions.

Bearing this in mind, the advantages of a specific license for Fintech companies are clear:

- Fintech companies would operate under regulatory certainty and supervision consistence.
- Regulatory burdens associated to applying for licenses on a state-by-state basis would be reduced.
- Fintech companies would have flexibility to decide their operating model, that is, to decide whether leveraging their services on existing banks or developing their own services from scratch.

16: Evaluating Charter Applications From Financial Technology Companies. OCC. 15 March 2017
17: DRAFT REPORT on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI). Committee on Economic and Monetary Affairs. European Parliament. 27 Jan 2017

On the other hand, specific licenses should ensure a better protection of the interests of customers and investors, a level playing field among incumbent banks and new entrants as well as more transparency and a better understanding of potential systemic risks associated with specific Fintech activities.

Overview of other regulatory approaches

Since the start of the Great Recession in 2008, higher capital and regulatory requirements have added to IT costs as (arguably) the main factors limiting innovation and availability of credit. This has created an opportunity for non-banking competitors to offer innovative services that fulfill unmet customer needs, although it has also raised concerns amongst financial authorities about the best way to increase the availability of funding and encourage financial innovation.

A typical strategy is unbundling banking activity in separate categories such as payments, deposits or lending and offering specific licenses and registration mechanisms for each activity. This approach increases the ability of new companies to provide banking services that are less risky by nature or that traditional banking institutions are not able to offer properly, boosting customer's satisfaction and choice.

The UK has pioneered this approach and subsequently emerged as the leader in Financial Innovation[18] thanks to a regulatory framework that supports financial innovation while keeping Fintech activities under control.

The EU also offers specific licenses for companies willing to focus on niche services. The landmarks are the licenses for payment and e-money institutions, created under the Payment Services and the Electronic Money Directives[19]. Both licenses allow new entrants to offer payment services with lighter capital requirements and offer a passporting facility across the EU, that is, the ability to offer authorized services in any Member State simply by notifying the Competent Authority of the country where services are to be offered. However, this approach in the EU is not final. The European Commission has recently launched a public consultation on Fintech that includes licenses among the addressed topics. The Commission is considering issuing guidelines regarding how certain business models fit under the current regulatory regime, issuing new licensing regimes at EU level or even a new "all-encompassing 'FinTech' license".

EU and UK legislation have influenced neighboring Switzerland and Turkey, which have enacted similar regulations. In fact, licenses for payment and e-money institutions have been in place since 2015 in Turkey. Switzerland has recently announced a new fintech license addressed to institutions taking deposits of up to 100 million francs that do not operate in the lending business. Switzerland has also followed the UK's lead, creating a sandbox facility that relaxes legal requirements for testing services under 1 million francs.

As far as the fast evolving Asian economies are concerned, both China and India have taken important steps to facilitate the access of Fintech companies mainly to lending and payment businesses.

18: See Fintech hub ranking in Ernst & Young, UK FinTech – On the cutting edge, February 2016;
19: See Payment Service Directive 2007/64/EC, the reviewed Payment Service Directive 2015/2366/EU and the electronic money Directive 2009/110/EC

Other countries such as Australia and Canada have joined the debate but are currently more focused on regulatory sandboxes and passporting agreements with countries as diverse as UK, Singapore, Kenya, South Korea, Switzerland, India or Japan.

The latest movement in this field comes from Mexico, where a proposed law on Financial Technology foresees new licenses for non-bank companies offering payments, electronic money, virtual currencies and lending.

Conclusion

As outlined above, the regulators' approach to Fintech companies differ greatly among countries. However, in order to reap the benefits that a seamless integration of Fintech companies in Financial markets can deliver, any regulatory strategy should encompass some features.

Firstly, it is important that regulators and supervisors take a proactive stance to balance financial stability and innovation, promoting competition and transparency. Authorities and Fintech companies involvement from early stages will ease communication, support Fintech development and allow Authorities to understand the needs of Fintech companies and identify potential risks at an early stage.

As technology is continuously evolving, it is important to avoid regulatory approaches that are too prescriptive. A dynamic, principles-based regulation which is as technology-neutral as possible and that includes incentives to innovate is imperative. Nevertheless, special purpose licenses should never exempt Fintech companies from complying with basic regulations such as data protection, security or anti-money laundering.

Finally, Authorities should factor in the global nature of technology and act in a coordinated manner, setting common standards and equivalent regulations while leaving room for the development of self-regulation and standardization initiatives at industry level. This is a major challenge due to the current competition among countries to attract FinTech businesses. However, international cooperation should strive for the creation of a level playing field among countries and market players, as well as for the implementation of smooth mechanisms, such as international passporting, that speed up the adoption of successful innovations.

5. Behavioural biometrics, a step further in digital identification for financial services

Growth of biometrics in the banking industry

As the world becomes more digital, financial institutions need to keep up with consumer demands. The use of biometrics in the banking industry has been gaining traction thanks to the arrival of devices that already include biometric readers and the expansion of wearable banking. The increasing scale and frequency of cyber attacks against user accounts in the past few years has shown that security cannot rely on identification means based solely on static biometric elements that can be compromised. Behavioural biometrics could be a solution to combating fraud and identity theft.

Passwords versus Biometrics

As a result of poor user experience, high and rising costs[20] and security breaches associated with the use of passwords, banks have been migrating to new digital identification systems that meet both the objectives of ensuring secure identity and improving user experience.

Biometrics is not uncharted territory for the financial industry; banks have explored options such as fingerprint scanning for decades, but the convenience and proliferation of mobile devices are making biometrics accessible to virtually anyone with a smartphone.[21] According to Goode Intelligence[22], by 2020 there will be at least 120 million customers using mobile biometrics on a daily basis for their financial transactions.

Biometrics use

There are two main types of biometric identifiers: **i)** physiological or static characteristics, based on the shape or composition of the body (fingerprints, iris, palm veins, face) and **ii)** behavioural characteristics, based on a person's behaviour (keystrokes, mouse movements, hand-eye coordination, hand tremors, navigation, scrolling and other finger movements).

Although financial institutions have been introducing different static biometrics for identification, **at present, fingerprint recognition systems are most widely used.** According to Deloitte[23] there will be one billion smartphones with fingerprint readers in use by the end of 2017. Nevertheless, by 2018, iris and face recognition will start to rival fingerprints. For instance, BBVA has recently started using biometrics for remote account opening in Spain, by verifying the customer's identity through a face recognition process. In India, project Aadhaar has captured graphic and biometric data of a billion residents in the largest biometric project of its kind in the world.

20: A recent survey of US companies found that each employee loses, on average, $420 annually grappling with passwords
21: Source: Biometrics: the future of Mobile Payments. Nathaniel Karp, BBVA Research, July 2015.
22: Source: Mobile Biometrics for Financial Services; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-2020. July 2015.
23: Source: A world beyond passwords: Improving security, efficiency, and user experience in digital transformation. Goode Intelligence. December 2015

Security issues

Hackers have figured out how to replicate the traditional means of authentication (SMS codes, tokens). Although static biometrics are relatively secure due to the fact that physical attributes are unique, it is also true that physical characteristics are **public, we cannot hide them and therefore they are easy to recreate and reuse.** Recently, we have seen in the news that hackers had tricked facial-recognition logins with photos from Facebook. In Japan, The National Institute of Informatics (NII) is warning that fingerprint recognition technology is allowing hackers to copy patterns from photos of people giving the peace sign. The consequences of a false positive can be very serious. Furthermore, when our biometric data is compromised, it cannot be used again and the damage is permanent.

Adoption of behavioural biometrics

Behavioural biometrics technology is able to learn patterns in user behaviour in order to build an identification model. The software analyses the way users interact with the different devices (phone, PC, tablets), how they hold the mouse, make keystrokes, how quickly they move, the pressure with which they hold the phone, etc. Over time, these biometrics are interpolated through algorithms and are able to define a unique pattern of each user in order to determine his or her identity in a certain way.

One element that differentiates this technology from static biometrics in verifying identity is that **the data is collected in a passive way and it does not interrupt the user activity, a key element for the user experience**

Companies like Google, with Project Abacus, are developing machine learning to authenticate users based on multiple assessments of their behaviour. The use of sensors, such as the camera, accelerometer, and GPS functions, allows smartphones to obtain a wide range of information about users, including their habitual geolocations, and how they type, walk, and talk.

Some banks have started to embrace behavioural biometrics as a replacement for passwords on mobile devices. One such bank is Leumi bank, an Israel-based bank that monitors users' finger size and the pressure of the user's touch to enable passive authentication. Some Fintechs, such as Mobetize, have also adopted behavioural biometrics to analyse the patterns of users and determine whether they are genuine customers, bots or hackers.

Legal Issues

As biometric technology is so new, there are **very few regulations that specifically address its use and application**. The biggest risk in the use of static biometrics relates to privacy issues, as readings are often stored in databases that can be compromised.

In Europe, regulators recognise that these technologies could improve user experience, but could also "lead to a gradual loss of privacy if no adequate safeguards are implemented"[24]**.** The new General Data Protection Regulation establishes that, for the processing of "special categories of personal data" such as biometrics, a higher level of user

24: Source: Data protection working party, Opinion on developments in biometric technologies, April 2012

consent – “explicit” consent - is required. Directives such as the new Payments Services Directive (PSD2) establish two-factor authentication for certain payments, where the use of biometric identification methods can increase the acceptance of mobile payments. The eIDAS Regulation calls for the optional use of biometrics to support eSignature applications throughout the EU. In the USA, some states have instituted regulations to protect the privacy of individuals’ biometrics.

In the case of behavioural biometrics storage, as human and interaction signals are collected, instead of physical biometrics, it is significantly a more privacy-friendly method.[25]

Conclusions

It is expected that banks will increase the use of these technologies, as they are becoming more accurate and easier to integrate into online and mobile applications. As single authentication methods are clearly vulnerable to attacks and it is where most of the fraud is taking place today, **banks are introducing behavioural biometrics as an additional way to protect the identification process. This approach allows the detection of anomalies in a customer’s patterns of usage after the authentication. It is the so-called multi-factor authentication.** By monitoring the patterns in a continuous way within a session, behavioural biometrics offer an integral solution to protect accounts from being taken over by hackers. The other factor that makes biometrics based on behaviour so attractive is user experience, as it works without interrupting the user’s daily activity in any way.

25: Source: Biometrics: The Physical Attributes vs. Behavioral Patterns Privacy Debate

6. The governance of technology in the digital world

Some emerging technologies follow an exponential growth and adoption rate and adopting them demands governance adapted to complexity and rapid change. In the case of the Internet, the model based on a combination of international cooperation and collective participation has so far –despite the internal debates– responded to the most significant challenges and may therefore serve a benchmark for governing other exponential technologies.

Governance of the Internet and its critical resources

The digital world is not independent from our lives; technological evolution is leading to a fusion between the physical and virtual worlds[26]. We cannot conceive of our everyday world without the internet, just as we cannot conceive of it without electricity. Internet access has been included in the Declaration of Human Rights since 2016 and, if that right is to be effective, it will require universal accessibility and affordability. Bridging the digital divide must be one of the objectives, but also internet use should be based on respect for human rights and democratic values. The Internet must guarantee citizens' ownership of data, and the protection of privacy and ensure diversity, pluralism and freedom of choice [27]. Protecting these values requires governance that is based on clear, inclusive and transparent rules.

Governance has been a subject of debate since the Internet's inception, and as the Internet has increasingly become the world's neural network, so the way it is governed has evolved. Compared to telecommunications governance models –the latest technological leap before the Internet– the contrast is radical, with centralized, often monopolistic models and strong state control, as opposed to the open and decentralized model that dominates Internet governance.

The start date of the Internet is usually given as 1969, when ARPANET was created; however, until e-mail and the TCP/IP protocol appeared in 1973, its size was insignificant; and even the in 90s, with the World Wide Web and hypertext, it barely reached beyond the scientific environment. The pre-eminence of this protocol over others, thanks to the "network effect" and its American origins, determined a governance model centred on the USA, which held sway until 2016 despite criticism and opinions in favour of a multi-stakeholder model led by the ITU (International Telecommunication Union). As the Internet grew, standardization processes gained more weight within the decentralized critical resource management model, and the outlook grew more complicated, involving many institutions in which the political powers had no direct representation but were seeking speedy technological action. We can see three layers in the digital governance: Infrastructure, logical layer and governance models.

The Infrastructure: the growth of the Internet has required the deployment of broadband lines over existing telecommunications infrastructures, with their own governance model, coordinated through the ITU (in which the

26: Shab, Klaus (2016), The fourth industrial revolution: what it means, how to respond, World Economic Forum
27: Overton, David (2017), Final report for The next Generation Internet initiative consultation, European Commission

private sector participates, in addition to 191 countries). The telecommunications sector is looking for greater profitability to obtain the return on investment required by extending the networks, while the **net neutrality** model (non-discrimination in data traffic) limits the attainment of part of the potential gains. While the European Union has spoken out on their behalf,[28] the current US government, which has not taken action against it, does not seem to offer much support.[29]

Because of the investment they require, infrastructure is one of the critical factors in bridging the **digital divide:** broadband coverage reaches two thirds of the world's population [30], but the new technologies require 5G networks in order to progress and allow access to thousands of devices on the Internet of things. The extension of these networks is already a priority for the developed countries [31].

The logical layer is managed by multiple independent actors that ensure the security and stability in a consensus-based approach.

- **Protocols and technical standards.** the institutions that currently govern these technical standards are:

  - IETF (Internet Engineering Task Force), founded in 1986 is an engineering group aim to develop technical standards under the supervision of IAB (Internet Architecture Board)
  - The Internet Society (ISOC) manage non purely aspects, as financial, fiscal and legal support to the IETF.
  - The World Wide Web Consortium (W3C), created in 1994 by Tim Berners Lee at MIT, created standards and recommendations to ensure the long-term growth of the web.

- **Domain name (DNS) and IP address management.** To operate the web requires a unique identifier for each address. In the early years these resources were managed in different ways until in 1998 ICANN (Internet Corporation for Assigned Names and Numbers) was created as a private non-profit organization based in California to manage domain names and IP addresses . Initially, ICANN was to report to the US government until 2000, but this mandate has been extended to 2016. In October of that year the transfer of IANA to the community of stakeholders was formalized. [32] There are also five regional agencies (RIRs) that manage the domains of each zone.

Governance: The debate between a US-centred model and organizations advocating a multi-stakeholder model (including ITU) took place in the first decade of this century. Some of the milestones are:

- The World Summit on the Information Society (WSIS), held in two stages (2003 and 2005), raised the importance of Internet governance as the basis for the Information Society, creating the WGIG (Working Group on Internet

28: Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access
29: Granados, Nelson, The FCC Hints At The Future Of Net Neutrality Under Trump, *Forbes*, 1 February 2017
30: ITU (2016), ICT Facts and figures
31: Véase por ejemplo: 5G for Europe action plan o A 5G strategy for the UK
32: IANA (2016), Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends

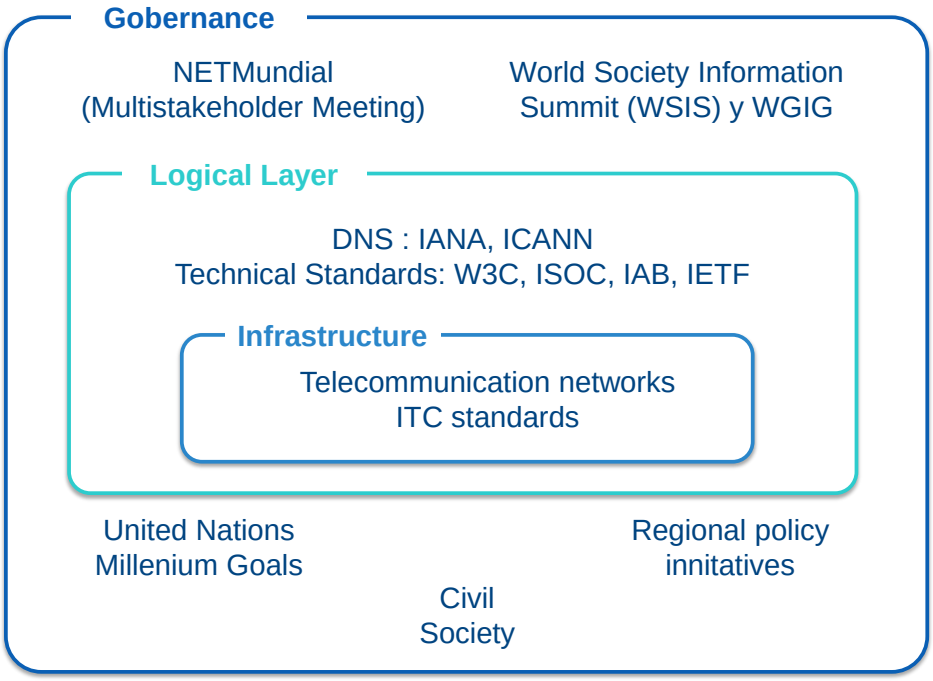
Governance). Other issues, such as reducing the digital divide, respect for freedom of expression and cybersecurity were raised.

- The Governance Forum (Internet Governance Forum, IGF): created in the second stage of the summit, involving all stakeholders. This aimed to internationalize internet governance. Its first meeting, held in Athens in 2006, focused on openness, security, diversity and access.

The governance model remains on the agenda with the upcoming celebration in April 2017 in Brazil of the Global Multistakeholder Meeting on the Future of Internet Governance (NETMundial)

In March 2017 the European Union published the findings of its consultation on "*Next Generation Internet*"[33], which lays great importance on the values on which the network is based, and the need for proper governance. Earlier this month China also released its *International Strategy of Cooperation on Cyberspace* [34], which affects security and cooperation in cyberspace and the need for a shared strategy.

Figure 6.1 The three layers of Internet governance



Source: BBVA Research, base don ISOC and The Royal Institute of International Affairs

From the earliest years, the digital divide, security, privacy, freedom of expression and protection of the rights of citizens (including intellectual property) emerged as the main challenges of governance. Part of the debate has shifted from the technical aspects of network management to the problems posed by **content.** Privacy and security are at the heart of the debate, especially in the wake of the Snowden case[35]. The increase in worrying phenomena – such as the

33: Overton, David (2017), Final report for The next Generation Internet initiative consultation, European Commission
34: International Strategy of Cooperation on Cyberspace, Xinhua net, 17 March 2017
35: In 2013, Edward Snowden, a former employee of the CIA and the NSA leaked documents on massive surveillance programs developed by NSA.

transmission of false information and using networks to express hatred– have led to new discussions about the freedom provided by the Internet versus the need for control.

The future: governance of exponential technologies

The emerging technologies are Internet-base, are growing exponentially, and the adoption rate is growing every more rapidly. The combination of different technologies and developments is taking us to a world of unprecedented change. Blockchain may be the new Internet; artificial intelligence and advances in robotics are giving rise to new moral dilemmas and a rethinking of the labour market. Virtual reality is blurring the boundaries of perception, while advances in biotechnology are bringing us closer to an unknown universe.

Maintaining technological advances with open protocols is a requirement if the development of new technologies, such as the Internet of things, is to safeguard the fundamental rights of individuals., The problems these new technologies face are similar to those faced by the Internet: the governance of infrastructures and standards, security, privacy, data control, the participation of civil society and the defence of ethical values.

Exponential technologies are global by nature, so a regulatory framework containing the minimum principles for development and governance that allows shared standards that respect values such as freedom, human dignity and privacy and encourage development of the technologies themselves is necessary. The world's largest companies are Internet-based, and therefore global. The growth of the digital economy requires a global technological and regulatory framework.

We can take the Internet as a model of exponential technology and governance, based on a combination of international cooperation and collective participation which, despite the internal debates, has, to date, responded to the main challenges. It should serve as a model in areas such as:

- Establishing open protocols, with standards governed by clear rules of competition, developed with the participation of expert communities. This openness allowed the triumph of the TCP / IP protocol.
- Extension of the infrastructure to develop these technologies, avoiding inequality.
- Avoiding a concentration of critical resources across distributed architectures.
- Ensuring that new technologies have an neutral regulatory framework.

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

The content of this document is protected by intellectual property laws. It is forbidden its reproduction, transformation, distribution, public communication, making available, extraction, reuse, forwarding or use of any nature by any means or process, except in cases where it is legally permitted or expressly authorized by BBVA.

BBVA | Research

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com
+ 34 91 537 36 75

María Álvarez
maria.alvarez.caro@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Edward Corcoran
Edward.corcoran@bbva.com

Jesús Lozano
jesus.lozano@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Ana Isabel Segovia
ana.segovia@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Macroeconomic Analysis
Rafael Doménech
r.domenech@bbva.com

Global Macroeconomic Scenarios
Miguel Jiménez
mjimenezg@bbva.com

Global Financial Markets
Sonsoles Castillo
s.castillo@bbva.com

Global Modelling & Long Term Analysis
Julián Cubero
juan.cubero@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Financial Systems & Regulation
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Countries Coordination
Olga Cerqueira
olga.gouveia@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Regulation
María Abascal
maria.abascal@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Spain & Portugal
Miguel Cardoso
miguel.cardoso@bbva.com

United States of America
Nathaniel Karp
Nathaniel.Karp@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey, China & Geopolitics
Álvaro Ortiz
alvaro.ortiz@bbva.com

Turkey
Álvaro Ortiz
alvaro.ortiz@bbva.com

China
Le Xia
le.xia@bbva.com

South America
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

CONTACT DETAILS: BBVA Research: Azul Street, 4. La Vela Building - 4 and 5 floor. 28050 Madrid (Spain). Tel.:+34 91 374 60 00 y +34 91 537 70 00 / Fax:+34 91 374 30 25 - bbvaresearch@bbva.com www.bbvaresearch.com