BBVA | RESEARCH

Digital Economy Outlook

MAY 2016 | DIGITAL REGULATION UNIT

Index

Summary

General Data Protection Regulation (GDPR): main issues and impact on financial institutions

The new General Data Protection Regulation (GDPR) will further harmonize the EU framework for the processing of personal data. Financial institutions will have to adapt their internal processes to comply with the new Regulation, which follows a risk-based approach and fosters a culture of accountability.

Tax challenges of the Digital Economy: the fiscal answer to the increasingly blurry frontiers for digital companies

In which country should value-added tax on online transactions be paid? Can we rely on the old definition of Permanent Establishment? There is an uneven playing field between foreign digital companies and local retailers. Meanwhile, millions of euros in tax revenues are lost every year. National regulatory initiatives arise and the OECD aims to reach a consensus

The Network and Information Security (NIS) Directive. Part 2 of 2

Continuing the previous article, in which we focused on the aspects of the Directive to be considered by online businesses, in this second article we look at how the European Union and, by extension, its Member States face a number of challenges, which are outlined here.

E-commerce in Spain: generational approach

E-commerce is an outstanding indicator of the importance of ICT in the economy. Electronic commerce has spread in Spain between 2003 and 2015, and a phenomenon of divergence is observed by age, emphasizing the inverse relationship between this variable and e-commerce. These results are amplified with the level of education.

Marketing in the digital era: adapting to the new consumer

Marketing is evolving in the digital age, just as consumers are. The supremacy of mobile phones and video in an attention economy changes the way that brands connect to customers, through content platforms, seeking to capture “micro-moments”, and by making full use of new data analysis tools.

1 General Data Protection Regulation

Main issues and impact on financial institutions

The new General Data Protection Regulation (GDPR) will further harmonize the EU framework for the processing of personal data. Financial institutions will have to adapt their internal processes to comply with the new Regulation, which follows a risk-based approach and fosters a culture of accountability.

Financial institutions are increasingly paying attention to the value they can extract from the large amounts of data they have access to: information self-reported by customers, transactional data that banks directly observe, internal operational data or information publicly available on the Internet. Big data and analytical techniques have opened a broad window of opportunities to increase revenues and reduce costs. By better knowing their customers, banks can anticipate their needs and offer them more tailored advice, products and services at the right time. Credit-risk assessment and fraud prevention may improve thanks to new analytics. Internal processes can be increasingly automatized and decision-making can be based on better evidence. Moreover, banks could provide intelligence services to third-parties, based on data analytics.

When analytics involve the use of personal data[1], regulation has much to say. Processing personal data is a highly regulated activity in most of the developed world, and particularly in the European Union (EU), where the 1995 Data Protection Directive set the general framework that has been in place until now. It will be replaced by the new General Data Protection Regulation (GDPR), a single set of rules directly applicable across the EU. This will further harmonize the EU regulatory framework, since national transpositions of the Directive have led to inconsistences between Member States.

After three years of intense negotiations, GDPR was finally adopted last month and will take effect two years after its formal publication.

Main issues in the new regulation

- The new Regulation creates a level playing field between firms established or not in the EU, since it extends its **scope** to organizations outside the Union when they offer goods or services to individuals in the Union or monitor their behaviour. Many of these organizations will need to appoint a representative in the EU. Moreover, data processors — not only controllers[2] — will be subject to direct obligations.
- The **consent** of the data subject remains the main legal basis for processing personal data. Yet obtaining it will be harder under GDPR, since it will have to be shown "by a statement or clear affirmative action", which closes the door for relying on "opt-out" mechanisms. The consent can be withdrawn, has to be specific to each data processing and the data controller is required to be able to demonstrate that consent was given.
- In the absence of consent, the "**legitimate interest**" of a controller may provide a legal basis for processing personal data, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Although the existence of a legitimate interest requires specific assessment, the "whereas clauses" mention fraud prevention and marketing purposes as possible grounds for a legitimate interest.
- The **rights of the data subjects** will be reinforced. In particular, individuals will be entitled to receive the personal data concerning them and, when technically feasible, to have such data transmitted directly from one service provider to another (a "right to portability"). Moreover, the existing "right to be

1: The new General Data Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable natural person"
2: The 'controller' is the entity that determines the purposes and means of the processing of personal data, whereas the 'processor' is the one which processes personal data on behalf of the controller.

forgotten" — set by the EU Court of Justice — will be codified in the new regulation. When an individual no longer wants his/her data to be processed, and there are no legitimate grounds for retaining it, the controller shall have the obligation to erase said data. Moreover, when the personal data to be erased have been made public, the controller shall take reasonable steps to inform other controllers that are processing the data.

- In line with the principle of **accountability**, some formal requirements are removed, but controllers are obliged to implement appropriate technical and organisational measures and be able to demonstrate the compliance of their processing operations. In particular, controllers must conduct a data protection impact assessment for more risky processing operations; keep record of all processing activities under their responsibility and notify data breaches — depending on the risks involved — to supervisory authorities and data subjects. Moreover, companies processing sensitive data on a large scale or monitoring large amounts of personal data will have to appoint a Data Protection Officer (DPO), in charge of assisting the controller or processor to monitor internal compliance with the Regulation.
- To reduce the legal risk faced by firms under such a principles-based regulatory framework, GDPR will introduce **certification mechanisms**. Accredited certification bodies will be able to certify controllers and processors on the basis of the criteria approved by the supervisory authorities. A common 'European Data Protection Seal' could also be introduced by the newly created European Data Protection Board.
- The existing regime for **international data transfers** will remain with no significant changes. The main ways for allowing cross-border transfers will continue to be "adequacy decisions" — by which the Commission recognises that a third country ensures an adequate level of protection — or implementing appropriate safeguards, such as binding corporate rules or model contract clauses. GDPR will remove the need for prior authorisation when transfers are based on certain approved safeguards.
- National data protection authorities (DPAs) will be in charge of **supervising** the application of the Regulation. In cases of cross-border processing, the lead supervisory authority — the one of the main or the single establishment of the firm — and the other concerned authorities will have to cooperate. The newly created European Data Protection Board, composed of representatives of the national DPAs and the European Data Protection Supervisor, will be in charge of ensuring consistency and will be competent to take binding decisions in case of disputes between supervisory authorities from different Member States.
- GDPR sets the maximum **administrative fines** that data protection authorities shall impose to controllers or processors in case of infringement. The most severe of these (e.g. breach of the conditions for consent or the requirements for international transfers) will be subject to fines up to 4% of total annual worldwide turnover or 20 million euros, whichever is higher.

Impact on financial services

Financial institutions will have to adapt their internal processes to meet the new requirements for obtaining consent; ensure data subjects can exercise their new rights; identify risky operations; improve traceability of all processing operations; and streamline the mechanisms to notify breaches. This will involve significant compliance costs. Moreover, given the risk-based approach of the new Regulation, firms are expected to rely on certification mechanisms to reduce the legal risk they face.

Finally, by further harmonizing the EU regulatory framework, GDPR should contribute to strengthen the Single Market for retail financial services, as intended by the ongoing European Commission's Green Paper. However, reaching an effective harmonization depends on the cooperation between all national DPAs and on the role of the European Data Protection Board to ensure consistency.

2 Tax challenges of the Digital Economy

The fiscal answer to the increasingly blurry frontiers for digital companies

In which country should value-added tax on online transactions be paid? Can we rely on the old definition of Permanent Establishment? There is an uneven playing field between foreign digital companies and local retailers. Meanwhile, millions of euros in tax revenues are lost every year. National regulatory initiatives arise and the OECD aims to reach a consensus.

The irruption of the digital economy is changing the economic paradigm and requires rethinking previous concepts and rules as they might not fit this new reality. This new environment brings both positive effects, like an increased customer choice and greater competition, and unintended consequences like reduced tax collection or an uneven playing field for local companies. Indeed, customers might acquire products and services from digital providers located in foreign countries where taxes are lower. This phenomenon is growing and regulators are adopting measures that should allow the maximum benefit to be obtained for all stakeholders, while still maintaining a fair competition. The Organisation for Economic Cooperation and Development (OECD) is aware of this situation: "Because the digital economy is increasingly becoming the economy itself, it would be difficult, if not impossible, to ring-fence the digital economy from the rest of the economy for tax purposes".[3]

What is at stake? The OECD's answer

The digital economy opens up the door for businesses to operate on a global scale. New business models and delivery channels arise and the traditional definition of direct or indirect taxes does not apply in most cases, as it is hard to determine which is the competent authority to comply with. These gaps in international rules reduce tax income and might allow shifting profits to low-tax locations with little or no presence of the company. The OECD refers to these activities as base erosion and profit shifting (BEPS) and has created an action plan to review current tax rules in order to reach consensus on how to approach this issue.

The Action Plan on BEPS[4] identified 15 actions, based on three fundamental pillars: introducing coherence in the domestic rules that affect cross-border activities, reinforcing substance requirements in the existing international standards and improving transparency. On Action 1, BEPS addresses the tax challenges of the digital age and identifies the main difficulties that the digital economy faces for the application of existing international tax rules. Their conclusions show the need to redefine how direct and indirect taxes are being established, while keeping the main principles of consistency, neutrality, efficiency, certainty and simplicity, effectiveness and fairness, flexibility, compatibility and consensus.

Direct tax applies to companies that are based within one country. To determine this, the Permanent Establishment (PE) concept is used to decide whether a company has to pay tax in one country or another. The challenge relies on how to decide where a digital business is located. A good example to understand this situation is the typical arrangement of global e-commerce sellers, where an internet provider can have its core businesses in one country, effectively invoicing from that location, despite using local warehouses to deliver the goods for their customers. Can we consider that the warehouse is a taxable nexus? Regulators are concerned by these organisational arrangements, and are aware of the potential use of those gaps in the interaction of different tax systems to artificially reduce taxable income. In this situation, a new definition of the PE concept is required to take into account three policy concerns that have emerged with the digital economy: nexus, data and characterisation of the income.

3: OECD. (2014), *Addressing the Tax Challenges of the Digital Economy, OECD/G20 Base Erosion and Profit Shifting Project*, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264218789-en
4: OECD. (2013), *Action Plan on Base Erosion and Profit Shifting*, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264202719-en

Indirect taxes or value added taxes (VAT) are also being affected by this new paradigm. One of the main consensuses achieved is that, for digital services, the place of taxation should be based on the place where the consumption occurs. However, this statement leads to further questions, like for example who is liable to account for the tax due and what mechanisms can be used for compliance and the payment of the tax due. Related to this, there is another issue to consider: the tax exemptions that most countries apply to small value goods at customs collection points, because administrative costs associated exceed the value of the VAT potentially collected. In the past this was a marginal concern, but with the growth of e-commerce VAT revenues have suffered a significant decrease and regulators are thinking of new systems to improve tax collection at national borders. A possible solution pointed out by the OECD in its Low Value Import Report implies reducing the cost of collecting VAT. Now, the issue at stake is how to avoid an unfair competition with national providers while keeping basic principles of international taxation, like avoiding a double taxation.

However, the biggest concern is related to the cross-border delivery of intangibles, like streaming content or applications. Those services do not enter the country through customs and might be contracted directly by the end user without the intervention of national intermediaries. Regarding this, OECD's E-commerce guidelines[5] recommend that the supplier registers, collects and remits VAT according to the rules of the jurisdiction where the customer is. This increases in complexity in terms of the process of selling abroad, but promotes local fair competition. However, this VAT registry is independent of the PE for direct taxes purposes.

EU and USA latest developments

Non-EU companies that want to operate in the EU can only declare PE in one member country for direct taxes purposes. In the case of indirect taxes of business-to-consumer (B2C) services, it is worth mentioning the creation of an optional scheme, the Mini One Stop Shop (MOSS) system. This scheme allows businesses that supply telecommunications, broadcasting or e-services to consumers in Member States in which they do not have an establishment to account for the VAT due on those supplies via a web-portal in one Member State. This foreign company will have to identify the EU countries where it has supplied that service and the VAT applied. The relevant tax authority will then split the amount among all countries involved. This regulation was established to create a level playing field among national and foreign merchants, as VAT applied is the local rate. If the provider decides not to use MOSS, it will have to register in each country where it provides services.

In the case of the US, this issue is also in regulators' agendas and many US states and cities are currently reviewing what measures should be taken, since there is no federal framework to cover all tax-related issues. As an example, the definition of taxable nexus, usually a physical presence, or the internet tax sales differs among states. To provide a common field, the Marketplace Fairness Act requires that states simplify their sales tax laws and grants states the authority to compel online and catalogue retailers ("remote sellers"), no matter where they are located, to collect sales tax at the time of a transaction.

New challenges: the example of 3D printing

Although there have been several advances made regarding international taxation of digital sales, there are still grey areas that must be assessed. A good example for this is 3D printing, where the final product is produced at the buyer's premises, even though the design can be made in any other place. In this case, deciding in which country the value creation took place that is to be taxed is complex. For 3D printing products, its value-added tax derives from its intellectual property (IP) rather than from its production costs. An obvious question arises: who owns this IP? However, once the 3D IP is owned and authorised for local

5: OECD. (2003), *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264103573-en-fr

use, an income might arise from that use that must also be taxed. The current VAT system is based on the notion that full value is delivered to the consumer, which is how it is taxed today. Capturing the full value of a 3D sale could be more challenging, as the product purchased becomes more intangible than tangible.

In conclusion, the digital economy is currently developing and further challenges related to it will surely arise. In this environment, regulators will have to find solutions to ensure a proper tax collection system, while promoting new business models and increased competition.

3 The Network and Information Security (NIS) Directive. Part 2 of 2

Cyber security regulation

Continuing the previous article, in which we focused on the aspects of the Directive to be considered by online businesses, in this second article we look at how the European Union and, by extension, its Member States face a number of challenges, which are outlined below.

In 2013, the Commission put forward a proposal for a Directive on measures to ensure a high common level of network and information security across the Union. Two years later, the Parliament and Council agreed on the text of the Network and Information Security (NIS) Directive.

Main challenges posed by NIS

The European Union and therefore the Member States, after several years of debate and public consultation, face a series of challenges, which are outlined below.

It is very likely that the transposition of the NIS Directive by each Member State could lead to different cybersecurity plans with different required cybersecurity measures in the different countries of the European Union. Today, there are varying degrees of cybersecurity maturity among the Member States and, as a result, the national transposition could lead to further fragmentation of the cybersecurity plan in each country. It is probable that some countries will apply a stricter interpretation than others, as occurred with the European Data Protection Directive (95/46/EC). This diversity of interpretation could lead to an unlevel playing field in the protection of consumers and businesses, depending on the requirements applied by each Member State, and it could be a barrier to companies that wish to operate in several European countries simultaneously. It is therefore important that there be one single NIS plan to cover the entire European Union and that there is a minimum baseline of identical requirements for all countries.

The small and medium enterprises that are not required to comply with the Directive will become the weakest link in the chain. It is also expected that software and hardware manufacturers will not be affected by the Directive, which is surprising since it would seem that they should be the first to meet the basic security and privacy requirements in the design of their products and services. The fact that all these companies are not subject to compliance with minimum security measures or the reporting of incidents could potentially create a scenario in which they could become a target of cybercrime. We should not forget that small and medium companies form the biggest percentage of companies using the NIS infrastructure. The European Union should perhaps impose a minimum mandatory set of requirements and even some kind of voluntary certification that would allow for differing cybersecurity maturity levels.

Some economic challenges need to be assessed according to the degree of maturity of each Member State, as there are already some countries with cybersecurity plans and even various national CSIRTs. It will also be important for ENISA to be provided with sufficient funds to coordinate the various national CSIRTs.

It is not currently known what the specific powers of a National Competent Authority (NCA) and National Computer Security Incident Response Team (CSIRT) will be. There is also no guidance on the overlapping reporting obligations under the various regulations, such as NIS and the future General Data Protection Regulation (GDPR). Similarly, no account has been taken of the possibility that some critical operators could be subject to simultaneous notification to various national and international regulators. For example, in the case of a Spanish bank, a personal data breach in a significant cyber incident must be simultaneously notified to the national data protection regulator, the competent critical infrastructure regulatory authority, the Ministry of the Interior and the European Central Bank. These challenges highlight the large number of

regulators that can be demanding the same responsibilities, creating regulatory duplication and, therefore, adding more complexity and costs for businesses and governments. A single notification mechanism in the style of a "one-stop-shop" could improve the effectiveness of notifications and reduce costs and complexity.

It is also a challenge to identify the most effective way to report incidents between entities and the standards to use, as well as to establish the same requirements in all Member States, thereby avoiding different implementations and obtaining a more effective sharing of incidents with public and private entities. It would also be desirable to contemplate a legal way to share incidents involving personal data, such as, for example, the IP addresses of malware-infected computers involved in phishing campaigns targeting public or private entities. In this way, the entities could be more proactive and obtain a significant reduction in cyber-attacks through effective collaboration between public and private companies.

Although the technical and organizational measures imposed on the companies affected by the NIS Directive initially do not require a product or service to be designed, developed or manufactured in any particular way, some countries might be tempted to impose a registration, approval or certification process for products and services. If the objective of such a provision was to foster a minimum degree of maturity in businesses, it would be essential for all Member States to reach an agreement, so as to prevent fragmentation. Possibly, a good choice would be to create voluntary but incentivised certification with varying levels of maturity, based on internationally recognized standards, such as the European Telecommunications Standards Institute (ETSI) or the IEEE-SA standards.

Conclusion

If necessary, the authorities with the power to transpose the NIS Directive could investigate and sanction cases of non-compliance. They must therefore have the power to make assessments of the level of cybersecurity and the measures required of company information systems. They could also require cybersecurity audits to be performed by third parties. In the absence of more information, there are concerns about what the requirements will be regarding minimum safety measures, whether they will be based on internationally recognized standards or audits, such as ISO 27001, NIST or SSAE16, or whether new standards will be created. It is also not known whether these standards and audits will be common throughout the European Union or if each country will adopt its own, leading to further fragmentation.

While the NIS Directive is certainly a major step forward in improving cybersecurity in Europe, we will have to wait and evaluate how the European Commission and ENISA will solve these challenges by enacting laws and guidelines, which are expected to provide greater detail regarding the implementation of strategic cooperation plans or the specifications and standards that may be used for NIS.

It is expected that in the coming months the Parliament and the Council of the European Union will formally approve the Directive, after which it will be published in the Official Journal of the European Union. Member States will have twenty-one months to transpose the NIS Directive into national law and an additional six months to identify the essential service operators.

4 E-commerce in Spain: generational approach

E-commerce in Spain by age and education

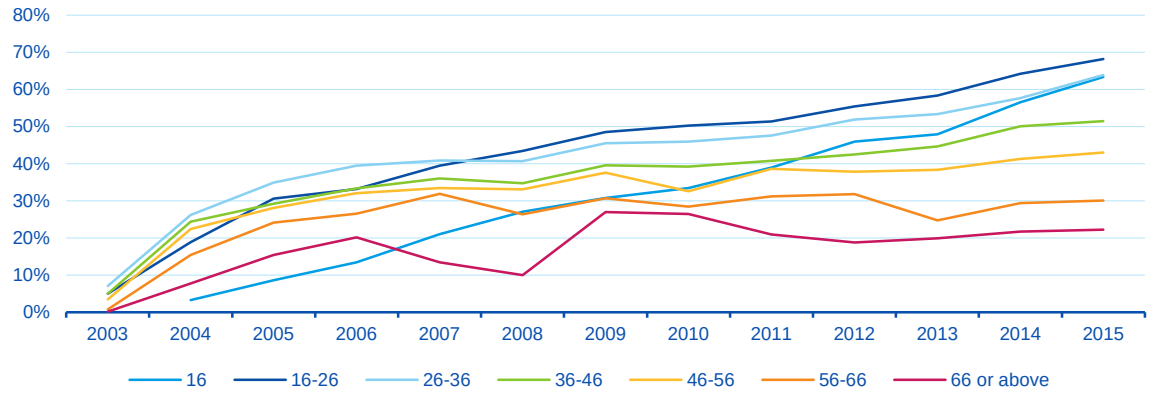
E-commerce is an outstanding indicator of the importance of ICT in the economy. Electronic commerce has spread in Spain between 2003 and 2015, and a phenomenon of divergence is observed by age, emphasizing the inverse relationship between this variable and e-commerce. These results are amplified with the level of education.

Consumer generations

Following the storyline of the November 2015 and January 2016 DEOs and using data from the ICT – Households (INE) between 2003 and 2015, several groups of consumers who use Internet (above 15 years old) have been created depending on age in 2003, at intervals of decades except for the last group, which includes people of 66 years old or above. Through this exercise, we can control for generations of Internet users and determine the evolution of them.

Figure 4.1 shows the behavior during the study period in response to the question of whether the respondent has ever used Internet.

Figure 4.1
Age distribution of e-commerce (%), 2003-2015



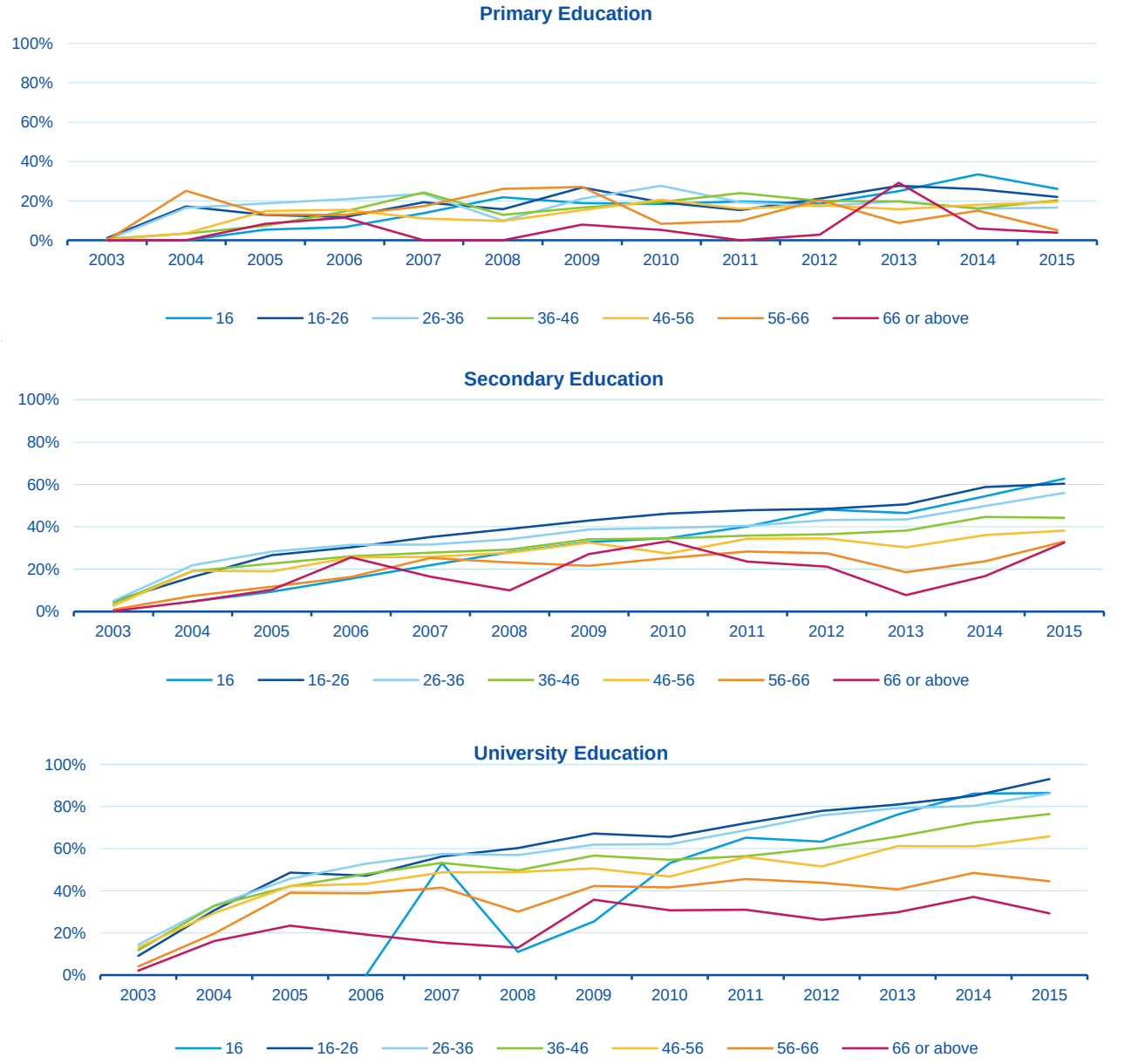
Source: BBVA Research based on ICT-Households (INE)

The results confirm the increase of e-commerce at all age ranges between 2003 and 2015, without appreciating clear signs from the economic cycle, as can happen with purchases in a more traditional format. All age ranges were based on a similar situation of scarcity of e-commerce activity in 2003, below 10 percent. However, the growth rate has varied among intervals, generating greater dispersion and the formation of three groups clearly differentiated. The most notable increases occurred among the population under 36, who have maintained the pace of growth in a sustainable way throughout the period considered, leaving the percentage of Internet users who have shopped online sometime in 2015 above 60 percent. The population between 36 and 46 years old form an intermediate group, with stronger growth in 2004 and 2005, and more attenuated in the following years, accumulating percentages close to 40-50 percent in 2015. Finally, those people over 55 years old have increased their percentage at a much slower pace and have undergone a process of stagnation since 2006. As a final result, the weights of Internet users who have shopped online for some time in these two older groups do not exceed 30 percent in 2015.

Education and e-commerce

As occurs with Internet usage, the education level is a relevant variable. Three levels are considered: Primary Education or lower, Secondary Education and University education. The results are shown in Figure 4.2.

Figure 4.2
Education and age distribution of e-commerce (%), 2003-2015



Source: BBVA Research based on ICT-Households (INE)

There is a positive relationship between the level of education and the percentage of people who said they had bought a product or a service online for some time, especially more intense the smaller the age of the consumer is. Thus, people with university degree have reached over 85 percent in the percentages under 36, while the weight is below 27 percent in the case of the primary education. The dispersion by level of education is much lower in the older population, varying from 30 percent in people over 66 years with university education, and only 5 percent for those with primary education.

5 Marketing in the digital era

Adapting to the new consumer

Marketing is evolving in the digital age, just as consumers are. The supremacy of mobile phones and video in an attention economy changes the way that brands connect to customers, through content platforms, seeking to capture "micro-moments", and by making full use of new data analysis tools.

Changes in the general landscape

Digital technologies, the widespread use of connected devices such as mobile phones and tablets and the predominance of social media, video and instant messaging platforms are transforming the way in which people consume information and therefore the way that companies need to target them to get their attention.

Today we are used to getting information simultaneously on a number of screens – watching TV with a tablet in your hand and the ever-present phone by your side. TV adverts have to compete with other digital content, meaning that these devices should also be targeted for advertising (the so-called inbound marketing).

'Attention economy' considers information as a subject that consumes our attention, something that is a scarce commodity in an environment where there is an excess of information. The time we dedicate to each piece of content is ever-shorter, and the battle for these micro-moments is a key factor for the new generation of advertisers.

Traditional media share the current stage with digital marketing tools, albeit with a different focus. Marketing via digital media has a greater capacity to better measure results and directly connect with consumer needs through the exploitation of data, unlike mass marketing through traditional media. The focus given to the two types of promotion should therefore be different, even within the same company.

The percentage spent on digital marketing has increased 24% in 2014 to 30% in 2016. The forecast for 2019 is that it will reach 35% of total expenditure for this area[6] in the U.S. Advertisements are the main source of revenue for search engines. The best tools in terms of positioning – SEO – were one of the most important new developments in the field of digital marketing. Nevertheless, this focus is not enough in a world of apps and social media, where the aim is to establish a conversation with customers and find out about their consumer habits.

The evolution of the consumer has led companies to focus on content marketing and brand positioning. Rather than design campaigns to promote specific products, currently the aim is to capture the consumers' attention with content that might interest them, which relate the brand to an experience and not to a particular product. The advertising that best highlights brand reputation should be integrated into the customer experience and adapted to their needs at any specific time and moment.

Achieving a correct measure of the conversion rate of digital campaigns is what allows optimisation of the budget. Today, instead of the traditional concept of ROI – return on investment, what have we spent and how much have we made? – what counts is ROMI – return on marketing investment. This takes into account the overall value that marketing adds to the organisation, including elements such as mentions on social media.

The attribution of the conversion rate to the correct channel is important in valuing a purchasing experience (known as the customer journey), which is developed though a range of channels. The most common situation is still the attribution of the conversion rate to the final channel, without taking into account the relevance of the other steps in the process. Although the tools used to measure the impact of campaigns are

6: VanBoskirk, Shar, *US Digital marketing forecast, 2014 to 2019*, Forrester, 2014.

evolving with the advances made through the analysis of big data, they are still anchored in ideas that stem from traditional marketing, which do not consider multiple channels or attribution as key factors.

The utilization of data has another evident use in achieving personalised attitudinal and behavioural segmentation compared to the traditional segmentation based on age and income level. Personalisation moves away from the use of mass campaigns that do not capture the consumer's attention, focusing instead on launching contextually relevant messages for a specific consumer in the place and at the time which is most likely to have the most impact.

The current **challenges** facing marketing managers are:

- Ensuring better use of **big data and advanced analysis** to improve measurement of results from campaigns and the deployment of information in the development of products which are increasingly personalised, replacing the current customer segmentation model and mass campaigns.
- The latest **technological advances**, which are changing the market, are mobile phone **ad blockers**. These programmes offer protection from intrusive or simply unwanted advertising, although they call into question the digital marketing business model.
- **Video consumption** is displacing an important part of companies' advertising budgets to platforms such as YouTube and the generation of viral content, which is shared exponentially via social media.
- The battle to attract consumer attention, which is increasingly fragmented into **micro-moments** and access to information through **mobile platforms**, requiring the generation of native content for this device which is easily shared through social media and messaging apps.

Marketing in the financial services industry

Spending on marketing represents an important part of the budget of financial institutions. Some relevant information, based on recent research into the American market[7]:

- In 2019, financial institutions will spend more than a billion dollars on digital advertising, while reducing expenditure on more traditional marketing media.
- Spending by type of device continues to focus on the computer, with 51.5% of the total budget, with mobile platforms accounting for the remaining 48.5%.
- The aim of campaigns is, above all, ensuring an increase in market share, loan growth and attracting new customers.
- In most of the financial institutions analysed, marketing is seen as a strategic priority, with the measurement of ROI considered to be of critical importance.

It is clear that the financial sector reflects general trends, although it continues to focus on campaigns aimed at specific products and not the brand. However, banks are adapting their apps and websites with a vision that centres on customer needs (“buy a car”) than generic product blocks (“car loans”).

As a reputation-building strategy, financial institutions can improve the financial education of your customers with content that is both relevant and highlights the brand. Digital campaigns, which seek brand positioning through marketing and the creation of content of interest to consumers, and also reflect the ideas of the institution but which are not direct product advertisements are becoming increasingly adopted by a number of financial institutions.

7: “2016 State of Financial Marketing”, *Digital Banking Report*, 241, February 2016.

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.

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

With the contribution of:

Francisco Borja Larrumbide Martínes
fborja.larrumbide@bbva.com

Alfonso Arellano
alfonso.arellano.espinar@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Developed Economies Area
Rafael Doménech
r.domenech@bbva.com

Spain
Miguel Cardoso
miguel.cardoso@bbva.com

Europe
Miguel Jiménez
mjimenezg@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

Emerging Markets Area

Cross-Country Emerging Markets Analysis
Alvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey
Alvaro Ortiz
alvaro.ortiz@bbva.com

LATAM Coordination
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

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

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Regulation and Public Policy
María Abascal
maria.abascal@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Global Areas

Economic Scenarios
Julián Cubero
juan.cubero@bbva.com

Financial Scenarios
Sonsoles Castillo
s.castillo@bbva.com

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

Contact details:

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