DIGITAL ECONOMY

An approach to the economy of personal data and its regulation

Javier Alonso, David Tuesta, Carmen Cuesta y Santiago Fernández de Lis

1. Introduction

The digital era's rapid change in the last few years has brought with it large-capacity data storage systems and new technological capabilities in information processing, at prices well below those at the end of last century. At the same time, the roll-out of latest generation telecommunications infrastructures is extending coverage throughout the world at breath-taking speed, bringing technology closer to individuals, companies and public institutions. Its consumption means that digital information is generated in volumes that are growing exponentially.

This mass of information, created through various channels, contains a large amount of data which is classified as personal; the sources can be contextualised information, pre-processed and structured data, but also from tracking, connection prints and an individual's internet browsing history. Inasmuch as this personal data is useful for both companies, since it improves their value proposition, and consumers, who receive direct or indirect advantages from the innovations and customisations which its use provides, a dense interaction with the data starts building up, which represents a challenge, not only for market operations, but also for regulation.

Thus, the personal data which forms part of an individual's private domain, and the circumstances in which their data has been captured, handled or transferred, are regulated in virtually every part of the world. However, the way in which the digital economy has been developing, and the new spaces where this information circulates and is shared, are cause for debate about how regulation is being implemented and the economic cost-benefit consequences. This point is the crux of this report, which aims to provide a conceptual view, with elements of regulation, technology and the economy, of data treatment and its implications for the privacy of individuals.

After this introduction, in section 2 we explain the potential exchange value of personal data, for both companies and for consumers. Section 3 looks at personal data exploitation from the economic perspective, trying to identify the various facets, and looking at the operating and regulatory challenges. Working from the economic scenario posited in the previous point, in section 4 we discuss current regulation, highlighting the most important ones in the United States and Europe, flagging up certain lines of action which may be helpful for the future. Finally, the study presents its conclusions in section 5.

Acknowledgements. We are grateful for the comments and suggestions provided by the BBVA Regulatory Compliance, Legal Advisory and IT Compliance departments, and in particular, the contributions made by Miguel Ángel Cañete, Miguel Marqués, Juan Manuel Matalobos and Jesús Alonso.

2. The digital era and the value of personal data

2.1 The value of personal data for companies

Personal information about the preferences, desires and needs of consumers has been exploited by companies to improve their results since the beginning of the 70s, when the market strategies which would end up influencing the entire productive process began to be developed most intensely. Even then, there were already several factors enabling firms to improve their results by using information about their customers' consumption habits as just another productive input. (Bailey, 1998; Bijlsma et al, 2014; Dayal, 2001).

The amount of personal information available in digital format is much larger now. According to IDC, a consultancy (in 2012), the digital universe is doubling every two years and will multiply by ten between 2013 and 2020, reaching 44 trillion gigabytes. A large part of this volume of information contains disaggregated data on individuals about their preferences, habits, characteristics and behaviour; thanks to the new technologies bracketed under the category "Big Data", it is possible to extract, process, organise and classify the information necessary to segment consumers by an unlimited number of variables that would formerly have been unthinkable.

Exponential growth in the volume of personal information online is due in part to the major technological companies which have arisen in the last few years, offering free digital services to end consumers; these include access to social networks, online search engines, email, data storage and photographs, etc., in which a large amount of personal information is handled. The global scale on which they operate and the success of the simplicity and innovation in their services has won them large market share and allows them to base their business model on offering third parties data about their users, generally through advertising spaces, constructing a business plan which can generate large profits. In this way, personal data about their customers not only helps companies to improve their own productivity, but also helps third parties, thus increasing the value of personal data.

This increase in the value of personal data is even higher when data from different sources is shared and cross-referenced, since it fosters the birth of new and innovative services. So, for example, if one knows where a consumer is from, their mobile phone and their consumption habits, one can present a product as the consumer approaches a business, even suggesting online financing to buy the item, if their credit history is also known. According to BCG (2012), the construction of services based on personal data could contribute profits to the public and private sectors of up to EUR333bn in 2020 (assuming an annual growth rate of 22%).

Personal information thus becomes a commodity with a significant transactional value for companies since: i) it helps to improve their productive process; and/or ii) it becomes a "raw material" for building new products and services.

2.2 The value of personal data for the consumer

The ever cheaper availability of fixed and mobile broadband, as well as the increasing penetration of mobile devices, has enabled a high percentage of the population to gain access to new sources of information, taking advantage of hitherto unimaginable digital services. These services are notable for being immediate and accessible from anywhere, at any time; on the whole they are provided to the user without a direct associated cost, beyond the connection to the telecoms networks themselves. Social media are a good example of this phenomenon, allowing users to communicate with each another and share all sorts of

information. Facebook has over 800 million users around the world who access their profiles every day, a further 1.28 billion who check it every month, and it generates an average of 1,500 updates a second.

It should be pointed out that most of the information available in the digital world has been shared by the users about themselves. According to IDC (in 2012), 68% of the information generated on the internet in 2012 was created and consumed by end users interacting on social media, emailing, storing photos, documents and videos in the cloud, among other activities. Using Eurostat figures, in the EU alone 24% of the population uses the internet to upload information onto the net and in some countries, such as Portugal and Denmark, the percentage goes up to nearly 48%.

As well as the personal data which users themselves publish, the net contains data which remains published sine die, such as public documents, digital press articles, messages, conversations and comments on forums. Users also leave footprints on the telecoms sensors and in browsers about their visits and browsing habits. Meanwhile, digital services manage, store and also process personal information about users' interactions: entries, searches, visits, purchases and electronic payments.

Thus, given the level of data that can be obtained about people by cross-referencing data from diverse sources, and depending on the use that is made of this data, users can see that their right to intimacy and privacy is crumbling. There has been debate recently about the use of personal data shared on Facebook, sparked by the revelation that user interactions in 2012 were used in experiments to research the spreading of emotion online (Kramer et al., 2014). Although Facebook has been warning users about their information being used for the purposes of research, and although users have supposedly given their permission beforehand – perhaps most have pressed "accept" on the warning without reading it or paying much attention - the members of the scientific community in the US stress that when behavioural experiments are carried out, the manner of warning people must be more personal, detailed and thorough, in compliance with the guidelines for the protection of human beings subjected to research (The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

Clearly, the perception of an invasion into one's privacy has a subjective component, which perhaps differs from one person to the next, giving rise to numerous inconsistencies in cases where awareness of privacy may be very high, and yet individuals expose their information without thinking twice about it (Acquisti et al. 2013; Acquisti et al. 2010; BCG, 2012). This is the reality behind the idea that, often, the individual is "selling" their personal information in order to access a service or receive something in exchange, but is not entirely aware of the subsequent treatment of their data. Perhaps one of the most interesting recent experiments conducted in the academic field is the one by Acquisti et al (2013), which examines the manner in which consumers assign a monetary value to sharing their personal data, when they are offered a sum which they consider appropriate. Acquisti (2004) had already put forward the idea of the existence of a preference for accepting the transmission of personal data by the individual in exchange for accessing a service or receiving a form of compensation immediately, as opposed to their bias towards protecting their data, which requires greater thought. For his part, Varian (1996) also indicated, back in the dawn of the internet, that people have different sensibilities about certain personal datasets being known. For example, he mentions that there are issues which people do not want to be made public (financial information, for example), whereas they are perhaps more tolerant about their telephone number or postcode being known, except when, as a consequence of the latter, they end up suffering some kind of annoyance, such as being "hassled" with unrequested sales information. On this latter point, Varian himself (2005) found that in the United States this sensation of annoyance about sales pitches varied depending on the individual's sociodemographics.

In any event, whether knowingly or unknowingly, personal data can end up becoming an instrument of exchange, bringing a range of benefits and/or damages. Acquisti (2010), Goldfarb & Tucker (2011) and Athey (2014) summarise most of these net benefits and the constraints faced by the consumer:

- If a product is acquired which has been specially chosen and designed for him/her, using their personal information, it is very likely to improve its utility, since it will optimise the value of the consumer's preferences.
- Personalised service provision, using personal information, improves the user's experience. So, for example, once a route indicator service knows the device's geo-location (and, as such, that of the user), it can redesign the optimal route to reach a destination every time the user changes the default route.
- The ease with which the sales proposition is received and purchased can save on search costs, once again increasing its utility.
- The possibility of companies improving their customer pricing discrimination depending on the latter's risk profile, in products such as insurance, for example, could once again improve consumers' overall wellbeing by means of two alternative routes. Thus, in the case of automotive insurance, the price of more prudent drivers' policies would improve considerably, since companies would be better able to measure their risk exposure. At the same time, drivers with more infractions would be discouraged from continuing their behaviour by the increase in the cost of their policy, due to their higher risk profile, thus reducing their level of risk, and the danger they pose to other citizens.
- The individual may experience some kind of discrimination in some markets because of revelations of their personal behaviour (good or bad), or some event in their past which is still in the public domain, despite a reasonable period of time having passed during which the person may have changed (Mayer-Schönberger, 2011). This was the reasoning behind the European Court of Justice's decision about the right for certain information of a personal nature which is inappropriate or obsolete to be removed from search engines, which became known as "the right to be forgotten" (European Court of Justice, 2014).
- The individual may want to interact freely on the internet, but feels threatened by the potential danger that a data leak or identity theft could damage their reputation or intrude on their privacy.
- An individual may also gain indirectly from greater knowledge of certain situations which help them to make better decisions, based on the analysis that others make of personal data. For example, the use of personal information for journalism, or a research centre or institution, whose conclusions are public.
- At the other extreme, there are also situations in which the use of personal data by national intelligence centres to improve a country's security (for example to prevent a terrorist attack), may be positively valued by a significant proportion of people and companies.

On the whole, following Bijlsma et al. (2014) and Varian (1996), ***people may feel comfortable with the transfer of their private data onto the web, depending on the use that is made of it, and the advantage that can be obtained***. Behind all these issues circumscribing the interaction between different players and their personal data, there are two key elements in which economic agents interact on the markets, as well as the legal and regulatory framework around them. We will be looking at both of them in the sections below.

2.3 Opportunities that personal data exploitation provides for banking

The banking sector has been one of the pioneers in client database management for the provision of financial services, in the areas of saving and credit. 30 years ago, a banking industry visionary said that "banking is only bits and bytes" (Skinner, 2014). Personal data supplied by customers to obtain certain financial services has been to a large degree the basis for creating credit histories, to evaluate the suitability of the financial customer using regulatory capital laundering standards, as well as to generate the supply of new products. In this digital era, managing customers' information has a central role in making services more

efficient for the different players active in the financial ecosystem. Below, as an example, we mention two areas which would gain from greater use of customer information.

Rating and scoring procedures

The procedures for assessing solvency, prior to being given a loan, could be improved if new variables from the internet were introduced, such as social reputation (of an individual or a company) or information in the public domain provided by states (concessions, resolutions, etc.).

If we look at qualitative variables we can view risk differently. Data such as the number of connections on LinkedIn or contacts on other social networks – in the case of individuals – or the number of visits to a website, the number of "likes", positive references, etc. – in the case of an electronic trader – seem destined to become new indicators that should be included in risk models. This does not mean that traditional analytical models based on historic information about the customer's credit behaviour should be substituted, rather that they should be complemented with purely digital information variables to complete the subject's risk profile.

Nevertheless, we should point out that despite the accessibility of the data obtained from public networks, this can easily be falsified, and as such should not provide much of a guarantee. What is clear is that this digital information becomes more useful when applied to subjects about whom virtually no qualitative information relating to their credit history is known. In fact, there are already credit institutions that are pioneering the use of digital social data for evaluating risk, such as Neo Finance (Palo Alto, California), Lenddo (Hong Kong), Kreditech (Germany, also operating in Poland and Spain) and MovenBank.

However, a degree of controversy exists around the application of these techniques to physical individuals, since some sectors consider that these activities may invade individual privacy. Around the middle of 2012, Schufa, the institution in charge of collating German residents' credit histories, had to abort the project it had commissioned from the Hasso Plattner Institute, of assessing the degree to which public information on the internet can help to improve consumer solvency. The pressure from consumer associations, supported by German law on privacy issues, was crucial.

The battle against fraud

Another banking procedure which is helped by the momentum of Big Data is in fraud management. Techniques to prevent and combat fraud use two approaches: i) via identification and authentication protocols to validate the customer's identity, and ii) through monitoring the customer's operations to identify illicit movements.

Monitoring movements and operations carried out using financial cards is widespread, with the use of data-mining techniques and artificial intelligence systems based on neural networks which learn from historical data to recognise fraud patterns. The increase in the processing capacity of cloud services and the new Big Data technologies allow a larger number of variables to be included in the monitoring, enriching the system by providing more accurate probability estimates as to whether an operation is fraudulent.

On the other hand, measurements of typing speed, access habits to particular webpages, or schedules or devices from which an individual connects, even how they handle a mouse or interact with a mobile device, form a pattern which makes it possible to authenticate an individual in an unobtrusive way, giving them a more user-friendly experience.

3. Economic theory, data privacy and interaction between parties

Advantages of the personal data market

Some of the experiments discussed, such as that conducted by Acquisti (2013), seem to confirm that personal data has a transactional value. Consumers can obtain direct and indirect benefits by providing it, while companies can use it to add value to their firm's activities. However, an economic approximation to the markets, where personal data circulates along different routes, tells us that there are several dimensions for analysis, which we will endeavour to cover.

Insofar as personal data has an economic value for companies, it can be traded in an organised and regulated market. Economic theory shows us that a perfectly competitive market is one in which the producer's and consumer's "surplus" is optimised, with this solution bringing efficient balance and the Pareto optimum. If the so-called "personal data" are traded on a primary market in conditions of perfect competition, it is understood that the balance will be reached by which both supply and demand maximise their positive outcomes. In the case of this hypothetical personal data market, the supply would be represented by the citizens, while demand would be represented by companies.

Going beyond individual benefits in a competitive market, an element of differentiation would exist as a result of massive sharing of personal data in the market, which increases still further the positive outcome for people and society. This is known in economic theory as network externality, understood as the increase in utility deriving from the use of a product when the number of people using it rises. That is, each additional user confers an extra benefit on existing users (Economides, 1996; Shapiro & Varian, 1999; Liebowitz, 2002; among others). The direct benefits derive from the interaction between users, while the indirect ones derive from the producers who, acting on economies of scale, have the incentive to develop new goods and services which are compatible with the technology. In the digital era, it is precisely this economic phenomenon which accounts for the benefits of greater participation in the worldwide web, where information that users find useful is shared, with social networks such as Facebook and Twitter being two of its principal benchmarks. On these social networks, as well as keeping one another informed, there are algorithms generated by these companies which provide a better selection or recommendation of services and products in line with individual preferences, which extends people's experience and as such leads to greater satisfaction. Network externality does not stop at social networks; it is precisely this greater participation on the part of people, with their personal data, which has been encouraging major development in all sorts of fields and industries. We referred above to how new financial players have been able to extend the supply of credit to new segments of the population, based on the analysis of this huge volume of personal data, providing them with greater growth opportunities.

Market faults in the personal data market

Whatever the benefits that a personal data market can bring to society, there are many elements which trigger market faults which stop it from working in conditions of perfect competition.

Market faults in the personal data market

1. Lack of education among citizens about personal data protection
2. Impact on consumer habits in the event of security breaches or inappropriate use of personal data
3. Privacy policies that are hard to understand
4. Regulation that reinforces the market dominance in data usage of large firms
5. Absence of metrics showing the net benefit received by the consumer when their data is shared
6. Regressive privacy norms

7. Difficulties in exercising the right to withdraw from the market

Lack of education among citizens about personal data protection

Many consumers are not sufficiently well informed about how to protect their personal data and do not understand the risks to and benefits of privacy, nor the conditions of use existing in the market (Athey, 2014). Furthermore, McDonald & Cranor (2008) estimate that an average American internet user will dedicate 201 hours a year just to reading privacy policies and warnings before giving his/her consent. This situation is made more complicated by the existence of multiple sector and local regulations, depending on the geographical area in question, which creates a situation in which the public at large, and even the experts, do not understand how governments and other institutions are making use of their data. When scandals about information loss or its illicit use are published in the media, users are not sure whether the organisations involved are following best practice or complying with current legislation in all its aspects, given that this information tends not to be public. This can generate a scenario in which the consumer feels powerless.

Impact on consumer habits in the event of security breaches or inappropriate use of personal data

Another factor stressed by Goldfarb & Tucker (2011), Tsai et al. (2011), Athey (2014) and Acquisti (2013) is the reaction which in practice the consumer has when scandals break in the media about inappropriate management of personal data. That is, it is difficult to learn their short-term perceptions, and much more so in the long term, when longitudinal experiments will have to be conducted. Some clues have been thrown up in the work of Goldfarb & Tucker (2011), who have found a “withdrawal” reaction, of more cautious behaviour patterns on the web on the part of users when cases of information leaks are publicised. Regrettably, this does not enable us to capture hypotheses relating to changes in perception between generations.

Privacy policies that are hard to understand

An interesting aspect about market faults in the world of personal data is signalled by Athey (2014), who shows graphically that many technological product markets are highly concentrated, and consumers do not really clearly understand the differences between the various privacy policies for equivalent services. For example, the ways in which the privacy policies are communicated, as well as the information clauses and user consent, cannot easily be assessed when there is no comparable alternative in another product. Furthermore, warns the researcher, if users have invested a lot of time in learning about and familiarising themselves with the application, it is difficult for them to move to another service when the privacy policy of the product they use has changed; and, furthermore, the consumer has no way of knowing whether the alternative service/competitor’s privacy policy has changed too. Therefore, the incentive for the consumer to penalise the firm for its unsuitable privacy policy is very low.

Regulation that reinforces the market dominance in data usage of large firms

With regard to the previous point, some positions state that it is the regulation itself that ends up most distorting the market. Athey (2014) shows that privacy policies can limit the development of new market ventures and thus curtail competition. In a similar vein, Campbell et al (2013) state that current regulation may be reinforcing the market dominance of major firms which use personal data, making it harder for new players to join the market.

Absence of metrics showing the net benefit received by the consumer when their data is shared

It is almost impossible, in real life, to calculate the net benefit to the consumer of sharing their personal data or not. In the case of privacy policies, for example, the supposed advantages they generate can neither be known nor measured consistently. As Athey (2014) points out, it is impossible to measure something which the consumer does not understand; on the contrary, one finds surprising situations in which some statements from different sources warn of the discomfort shown by people in the presence of personalised sales pitches based on their email information, but at the same time these companies' earnings continue to rise as a result of using these practices. We saw in section 2 that the papers by Acquisti (2013) and Varian (2005) found that the perception of greater or lesser benefit on the part of the consumer in the use of their personal data depended on the context. As such, this situation makes it very complicated to consider regulatory policies that can be applied across the board.

Regressive regulations on privacy

Also following on from the previous point, it is interesting to note that privacy regulations can end up being regressive. Athey (2014) finds that in many cases the regulation covering on-line sales announcements affects the advertising of the so-called free access products, which are precisely those most appreciated by people on low incomes, by students and by small business. In one example, Miller & Tucker (2011) found that in the case of those US states which adopted the strictest privacy policies, they reduced the adoption of electronic medical filing systems, with a resulting increase in child mortality, particularly among the lower income groups. A clear example of the law of unintended consequences.

Difficulties in exercising the right to withdraw from the market

It is necessary to guarantee the right of all citizens not to participate in the market if one of their preferences is not to do so; in other words, the market should not have entry or exit barriers. As we saw above, on the internet the "right to be forgotten" has recently been the object of a ruling in Strasbourg against Google (European Court of Justice, 2014) which guarantees citizens the option to demand the removal of certain obsolete and/or inappropriate information susceptible to being picked up by a search engine.

On the whole, we can see that the existing faults in the personal data markets lead to solutions which are not ideal for the agents interacting in these markets, altering the net benefits that might be expected for society of absolutely correct use. We have also seen that these facts, which clearly justify the regulator's intervention, particularly when we consider that the right to privacy is a universal right, lead to less than ideal solutions. What does the current regulation consist of? What routes for improvement can we see? We will discuss this in the next section.

4. Regulations in the area of privacy

4.1 Characteristic features of regulation on the law affecting privacy and personal data protection

Privacy is considered in Article 12 of the Universal Declaration of Human Rights (1948) and in Article 17 of the International Pact for Civil and Political Rights (1966), as well as many other international and regional Human Rights treaties. Practically all countries in the world include the right to privacy in their constitutions, regulating the relationship between states, public and private institutions and citizens with respect to their right to privacy and personal data protection.

Although concerns about privacy have a long track record, it was at the end of the 80s and the beginning of the 90s, when the roll-out of what were then new information technologies began, that society was alerted to

this exposure of its private information. Communications networks made it easy to transfer information between places far away from one another, and the large mainframes were capable of processing major data volumes. Technological evolution has now exponentially increased the capacity to interconnect information, which can make it possible to assemble an exhaustive profile of an individual.

Europe

Europe has the most developed privacy of information and personal data protection regulations for its citizens, complying fully with the OECD principles (1980). In 1995 Directive 95/46/EC was passed in Europe, "on the protection of individuals with regard to the processing of personal data and the free movement of such data", with the aim of harmonising national regulations and setting up some common principles which would facilitate the creation of the European Single Market. Information flows between member states were thus permitted in a context of consumer rights protection, preventing this flow to countries where appropriate protections were not in place. This Directive and the OECD's guidelines have also inspired regulation on other continents. So, other geographies are obtaining a comparable level of protection that can be assimilated with Europe's, under which data transfer from Europe is allowed, in order not to put barriers in the way of inter-regional trade.

United States

Regulators in the European Union and those in the United States have held very different positions on the development of the legal framework around their citizens' personal data protection and privacy. Whereas Europe has placed the spotlight on arbitrating all the occasions when personal data are handled, in the United States there is a plethora of state and nation-wide norms which are applied sector by sector to those industries which handle the most sensitive data, as is the case with the financial and healthcare sectors, and also information about minors.

In the case of the US, and despite the impact of the introduction of the European Directive on US companies with a presence in Europe, the initiatives to introduce a similar regulation were thrown out in favour of encouraging innovation in an increasingly digital world, in which personal data is the input around which new businesses rotate. Thanks in part to the freedom with which US firms sprang up and have been developing their usage of their customers' data, major technological firms have appeared, such as the likes of Google, Facebook, YouTube, Twitter and Groupon, all of which base their business models around online advertising based on the profile they obtain of their users. This exclusively sectorial approach has helped to create spaces in the system which allow new digital companies to enter, and to provide services and applications which were previously the prerogative of other industries, which by their legal nature are subject to the precepts of legislation, all of which implies a contrast between the two regions' regulatory realities.

4.2 Routes for regulatory improvements in a global context

Conceptually, regulations on privacy and personal data protection ought to meet a series of criteria which fulfil the expectations of economic agents. On the one hand, some consumers want to put a value on their information and for it to be well managed and protected. On the other, companies want to use this same information for their productive process with as little friction as possible, in a balanced regulatory environment between consumers and firms, which enables them to contribute to the innovation process. That is, regulation needs to be structured so that it can reach a more competitive type of environment in which both consumers and producers together maximise their utility and profit, which will bring a positive outcome to society.

Ways of improving data protection regulation:

1. Continuous updating of regulation

2. Standardised and simplified privacy policies. Towards segmentation of the data market
3. Appropriate authorisation processes
4. Pseudonymous data consideration
5. Better balance in the accountability between data generators and data users
6. Certifications of good practice in personal data use
7. International cooperation

Continuous updating of regulation

The speed of change in information processing is such that regulatory approaches to privacy and personal data protection are becoming obsolete. There are swathes of national and local norms which are not designed to operate in an ecosystem in which information flows between different regions and continents. Services that can be accessed from anywhere, at any time, and are increasingly in demand, proliferate in direct proportion to the availability of high-speed networks and mobile communications access, which give access to a digital world in which the participants (users and organisations) may be subject to very different legislation from one another.

For example, the following events are very likely to occur simultaneously: i) an increase in the demand for personal data information; ii) a change in user perception on the part of new generations, who are more inclined to transfer/sell more personal data (changing perceptions of privacy), and iii) a regulatory framework which continues to uphold the same position vis à vis people's wellbeing. This combination of effects might produce a loss of both efficiency and that very wellbeing, which a suitably dynamic set of regulations ought to avoid.

Standardised and simplified privacy policies: towards segmentation of the data market

One way of creating the right climate for achieving a competitive market is to segment it into sub-markets which bring demand closer to the characteristics of the supply, so that it is easier to adapt to competition. In this case, citizens will be able to offer or restrict their information, depending on their preferences, to a range of uses which differ from those of the normal market, and receive for it a price/service differentiated by demand. The fact that regulation allows supply to have control over its own segmentation helps to bring a competitive scenario closer, which in theory will generate greater wellbeing.

For this to happen, it is crucial that regulations exist to standardise and simplify privacy policies so that they can be properly understood, and that market incentives be introduced so that the user has the option of sharing these policies and deciding between them, at the same time as spaces open up to incentivise the user or sanction the infringer, as the case may be. However, as we pointed out earlier, a good privacy policy is not the only thing users see; they also bear in mind the cost to them of giving up the time invested and the familiarity won with a service/product. Segmenting markets is a good route to go down, but these other aspects which some users may value more highly, and which could reduce the effect of the regulatory policy enacted, need to be factored into the calculation.

Appropriate authorisation processes

Current formats for acceptance of, and consent to the use of, personal data have a high cost in terms of reading and comprehension on the part of the users. This may give rise to circumstances in which users may be accepting, by default, the conditions imposed on them by the provider. Later, this consumer notices the implications of this acceptance (for example, receiving advertising not appropriate to their tastes; or finding out about a way in which their data is being used of which they were unaware), which will lead them to distrust the system.

The regulation ought to make it possible to compose standard forms on the acceptance of personal data use which are straightforward, swift and easy to understand. From a theoretical perspective, Campbell et al. (2013) propose the creation of a profile of personal data use acceptance which is conducted only the first time, and which can be used by any company or ITC application in the world, thus bringing down the transactional cost of the economic agents who have to obtain authorisation every time they request access. Another approach could be to allow greater control over the individual's own data, by means of mechanisms which enable them to decide how their data will be managed, throughout the life of the contractual relationship, which would add greater transparency and could generate trust. Apart from the advantages which each of these approaches could have, the core challenge continues to be an increased likelihood of the user actually reading about, amassing information on and becoming aware of what is happening.

Pseudonymous data

Another important issue that has to be tackled is the treatment of some personal or pseudo-personal information which identifies the person, and as such is protected under current regulations. Although it is true that digital technologies allow one to identify the physical person using data that is not, a priori, personal, such as browsing traces, or by recognising devices from which they browse, the generation of profiles and behaviour patterns and their exploitation, disconnected from the personal identifiers, continues to generate high value for companies and, in the final reckoning, for society. The introduction by the European Parliament of pseudonymous data in its review of the new privacy regulation (still pending approval), together with the relaxing of the regulatory burden on this data, appears to be an initiative which meets the need to allow companies greater flexibility with data treatment without trampling on the fundamental rights of individuals.

Better balance in the accountability between data generators and data users

We have pointed out above how one of the main problems is that as individuals we are frequently unaware of the authorisations that we give for the use of our personal data. The boxes with notifications and warnings that frequently appear when we interact on the web are often ignored, quickly accepted so that we can carry on browsing. Many experts believe that this is because the texts are long and complex, but some anticipate that making them simpler would not mean that a major slice of the population becomes more aware and seeks to learn about them. This problem is more complex in the Big Data era, now that it is difficult to explain to people the exact use to which the information will be put, as well as the complexity of the experiments and consequences of these on their future wellbeing.

In the light of the above, many experts recommend a better balance between the responsibility for how personal data is used, so that not all the weight falls on people. Mayer-Schönberer y Cukier (2013) and The Centre for Information Policy Leadership (2009), for example, suggest that this accountability should be apportioned to those exploiting the information. That is, "notifying" people and "waiting for their consent" appears not to be enough in the era of Big Data. To a certain degree, it seems sensible to transfer greater responsibility over to those using the information, given that they know much better than anyone else – and definitely much more than the consumer or the regulator - the intended use of the data. Experts' recommendations for this greater weight of responsibility on the data analysts are that the latter should be required to conduct a risk analysis on the data use, not only the first time, but on subsequent occasions. Although this may be costly for some, it could be mitigated if the regulator indicates what type of data or situations require this risk analysis. If this risk analysis is done well, companies could save themselves the costs of asking for consent every time they want to use this data, since the latter will have been studied before.

Not only ex-ante protection but also ex-post: regulating the risk that the predictions on the basis of personal data are crucial for people.

The problems with using personal data not only need to be controlled for ex-ante but also ex-post. Following Mayer-Schönberger (2011) and Mayer-Schönberger & Cukier (2013), in the Big Data era and the predictions which its complicated algorithms throw up, the world is gradually tending to use them as determinist markers. In several situations, the use of likelihood scenarios which throw up personal data exploitation within the Big Data system has been of some help, for example, in reducing crime in some cities. Today over 50% of conditional liberty recommendations in the United States use predictors based on Big Data techniques as a decisive factor as to whether someone walks free or not.

Exploiting personal data poses ethical and moral questions about the human condition, which will require a lot of further development in future regulations.

The “algorithm monitors” and certifications of good practice in use of personal data

The fundamentals which underlie those algorithms which are used in exploiting personal data are of such complexity that people will never understand their range of consequences. Mayer-Schönberger (2010) and Mayer-Schönberger & Cukier (2013) discuss the possibility of introducing the role of “algorithm monitors”, scientists who audit algorithms, in the definition of the regulations and in the design of supervision over personal data which creates a fair balance between people on the one side and efficiency for society in terms of information use on the other.

These experts recommend that society should use this type of specialist to certify how these data are used. Algorithm monitors may be experts in the areas of computer sciences, mathematics or statistics and will work as auditors of Big Data analysis and predictions. They will take an impartial and confidential position in their projects, in the same way as accountants and other professions do now. Following Mayer-Schönberger & Cukier (2013), the algorithm monitors would assess the choice of data source, the choice of analytical and predictive tools, including algorithms and models, as well as the interpretation of the results. The role of the algorithm monitor could be key in providing a balanced market solution for all the economic agents, instead of excessively intrusive regulatory systems. To do this, there might be a role for external and internal algorithm monitors. This would enable the external algorithm monitors to handle government requests in situations which require Big Data predictions to be reviewed or validated. They could also be certifying companies, whose verdicts would be binding for regulators and supervisors. The creation of professional bodies of algorithm monitors could be considered, with members, just like doctors, lawyers, architects and other professions, who are subject to strict conduct and ethical codes in their activities.

Another idea would be to establish internal algorithm monitors within organisations to monitor in situ the activities being conducted with personal data, protecting in particular the interests of people who might be affected. There would be an algorithm ombudsman, to make sure that the entire data handling process, from the moment the data is obtained, up to the final outputs, is managed using ethical and scientific good practice. Naturally, all these actions will need to be proportional, to avoid their becoming costly processes which hinder technological process.

International cooperation in regulating personal data protection

In the global digital era, there needs to be a shortening of distances between international regulators so that basic and shared rules of the game can be defined for personal data treatment, allowing them to flow, but ring-fencing the individual’s right to privacy. A good approach is the work being developed in Europe to create a set of regulations covering all member states equally, as well as a single central supervisory institution for all. The European Commission estimates the profits of this integration at EUR2.3bn a year.

But a global market goes far beyond what happens in individual geographies. Market interaction and the data circuit happen around the world and we are now seeing digital companies of all sizes springing up on one side or other of the Atlantic or the Pacific, offering their services to the opposite sides of the world. With this in mind, regulation evidently has a very long way to go.

5. Conclusions

With data playing a central role in society's technological progress, its potential transactional value and the oversight regulation are crucial. It seems obvious that if we manage to reach an equilibrium at which the interests of consumers, firms and regulatory principles are aligned, the gains for the economy and the boost for innovation will be significant. Nevertheless, what we see is a world where market faults predominate and where the role of regulator, frequently a very paternalist one, can end up giving rise to inefficient solutions.

It is true that the universal principles that are the mainstays of the right to privacy must be respected and defended, not negotiated. The emphasis could perhaps be centred on that rather fuzzy frontier between what each person may consider private, and the opportunity costs that they themselves pay, with a regulation which allows everyone a margin of choice, without giving up the principles of good stewardship of our personal data.

We have discussed these issues, presenting the economic problems of personal data, the regulatory framework and the interaction between them, and then covered the real context of markets with all their imperfections. We have seen that there are many problems facing the data owner who seeks real information of the way in which their data are used, whether by governments or by institutions. We have also seen the difficulties in creating privacy policies which users are interested in reading, understanding and choosing. There is much evidence to support the assertion that people do not take enough time to read and understand very simple announcements, and that it is simply the confidence in the service from which they obtain value and with which they have invested a lot of time in becoming familiar, which carries more weight in their decision. And it is this very factor, taken with the market dominance of some of these service providers, which raises the barrier to entry for new players, which in turn makes it difficult for people to choose, reward or penalise those who have the best/worst privacy policy practices.

These circumstances, obviously, represent a good case for regulatory intervention. The problem is that in many cases the regulation is incapable of measuring the net effects on people's welfare and, worse still, of discerning who benefits and who does not. Regulatory interference may even mar the benefits which sharing personal data can bring society, as a result of the network externalities that are generated. We have also given illustrations some of the paradoxical situations that occur as a result of regulatory good intentions and, unfortunately, their negative results, generating harm in many cases to the most at-risk segments. We have also seen how some data protection practices, without meaning to, end up increasing the market power of the first entrants, now big firms, to the detriment of new ventures.

Nobody ever said that regulating this market would be easy, but that does not mean that nothing should be done. Regulation is facing a new and complex scenario, with lots of momentum on several fronts. Perhaps the most interesting thing is the generational factor, which may trigger a change in perception as to the limits of what is and is not private. These changes may lead to regulation as we know it having to adapt to new times, as regulations in other fields are doing. Adaptability and flexibility will perhaps have to be explored over the years. We must not forget a key component of our economies and societies that is inherent in these trends: the global factor. The digital era today lays out a scenario of integration, where frontiers and geographies almost disappear in the exchange. To continue with fragmented technologies does no favours to technological progress and to the positive benefits it has on society.

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.