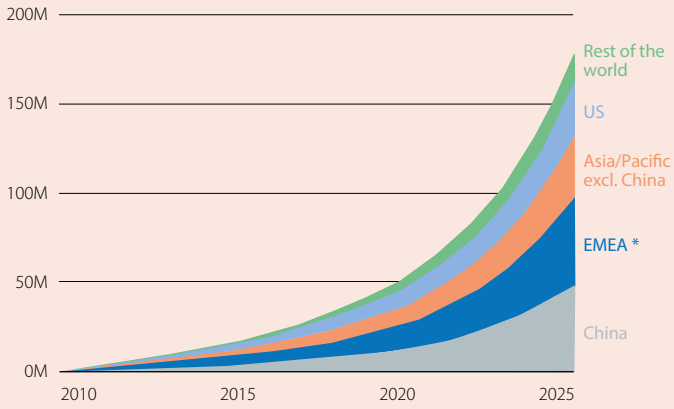
The data revolution: competition and responsible use

In recent years, the importance of data for the economy has become even more evident (see first chart). With digitisation, everything we do leaves a trace on the internet. When, for example, we open a mobile app or make a purchase online, we generate data that detail what we have done or where we have been. In fact, it is estimated that more data were generated in 2017 than in the previous 5,000 years.[1] In other words, the digital world is becoming increasingly capable of accurately describing what goes on in the physical world. This abundance of digital information, together with the use of new technologies – such as greater computing power – that make it possible to get more out of the data, generates significant competitive advantages for all the companies that know how to make use of it. However, this intensive use of digital information is also the focus of many debates because, inter alia, it raises fundamental questions about data ownership and privacy.

In this article, we look at two key aspects that emerge with the use of digital information by firms: on the one hand, changes in the nature of competition, and on the other, responsible and ethical use of data and of artificial intelligence.

Global data growth

The volume of data has increased exponentially in the digital economy and will accelerate over the next decade (Zettabytes)



Note: ** EMEA stands for Europe, Middle East and Africa.*
Source: *CaixaBank Research, based on data from the Bank of England («The Future of Finance»).*

On the nature of competition

- **Data, in themselves, are non-rival assets**. That is to say, they can be used simultaneously by different parties without the amount of data available for the rest being affected. For instance, it is technologically possible for all researchers in the field of medicine to use the aggregate stock of medical data of patients at the same time. Due to this non-rivalry, the exchange of data flows can convey enormous benefits for society.
- **The ability to extract value from data provides significant competitive advantages**. Data, in themselves, have no value: the challenge is converting that information into value. In other words, it is useless to have data from millions of interactions if this information cannot be used to better understand the consumer or user, to find out what they need or how to improve their customer experience. However, converting information into value requires specific capabilities. These include having an adequate infrastructure to store and process the data, experience in data analysis and having specialised talent (capable of posing the right questions and articulating the answers to such questions).
- Given that data can provide major information advantages over competitors, companies do not have incentives **to share the data they have accumulated with third parties**. In this context, information can become concentrated – and disproportionately so – among a relatively small number of large companies.
- In addition, the **joint exploitation of network effects and large amounts of information can amplify the position of market dominance held by some firms**. This explains, for example, why large technology firms can process such vast amounts of data. In particular, the more users a digital platform has, the more attractive it is for other users to register and to operate on that platform – the so-called network effect. As the platform in question amasses more information about its users, it is in a better position to improve its products and services and to attract even more users (thus widening its competitive advantage over rival companies and consolidating its dominant position in the market).
- **The accumulation and intensive use of information** offer the possibility to come to dominate a market through the success of a product or service. In this case, there is a risk that this position can be abused in order to undertake anti-competitive practices. In this context, **it is important to ensure that it is possible to enter or exit the market with ease – the so-called market contestability – and to prosecute any anti-competitive behaviour.**[2] Unfortunately, **identifying and proving cases of abuse of market position**[3] in this new digital environment **is no easy task**. Among other reasons, this is because the position of dominance can be established relative to other competitors, rather than to the traditional consumer,[4] and because the line

1. Bank of England (2019). «The Future of Finance».
2. Competition incentivises firms to become more efficient, to innovate and to constantly improve the quality of their products and services. It also directly benefits consumers, who can enjoy a wider range of goods and services, which are of better quality and at lower prices.
3. The abuse of a dominant position occurs when a company that holds a dominant position undertakes any commercial conduct that is considered to be abusive.
4. For example, some digital platforms operate as intermediaries, while at the same time holding a position of control over the infrastructure that their rivals depend on.

between legitimate practices and anti-competitive practices is not always clear cut. As an example, digital platforms have a clear incentive to prioritise growth above profits, hence low price strategies become particularly important. However, establishing artificially low prices in order to drive a competitor out of a particular market is a practice that can be considered abusive. Furthermore, it is sometimes difficult to clearly determine the relevant market in which an abuse of power can occur, given that the boundaries of the market in which digital service providers operate tend to be blurry.[5]

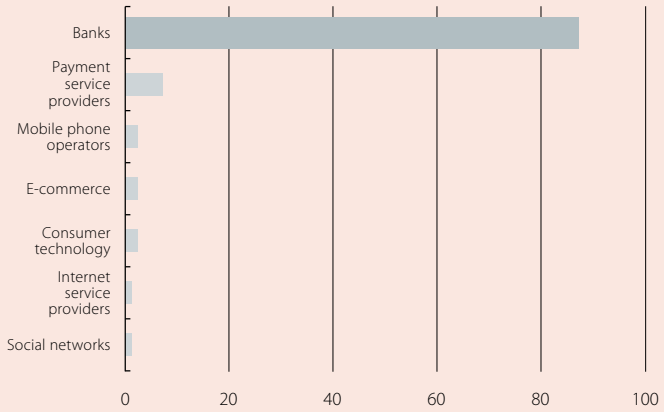
On the responsible use of data

- **Although there are different ways to extract value, the responsible use of data must be present in all of them**. The ethical and transparent use of data is an area that is attracting ever more attention from consumers and society in general, especially following several cases of misuse of personal data and as the use of digital information and artificial intelligence models by companies becomes widespread. In this context, ensuring that companies operate with ethical criteria and that individual rights are guaranteed is vital for maintaining society's trust in digital services.

- **Within this area, one of the most important issues has to do with confidentiality and data protection**. In particular, data are generated by users when using digital services, but they are used by firms and online service providers, which sometimes fail to properly respect consumers' privacy.[6] In addition, the consumer is often unaware of what data are collected about them and for what purposes, and they have no control over their use. On this note, there are studies that show that it would take the average user up to 76 days to review all the terms and conditions they accept in just one year.[7]
  - In this context, it is **important to find mechanisms that help consumers better understand how their data can be used and which tools they have at their disposal to protect their privacy**. In this regard, the EU is at the forefront when it comes to establishing clear rules on data protection, following the entry into force in 2018 of legislation that seeks to ensure that the consumer retains control over the information they provide.[8] On the other hand, in the US, an increasing number of voices both inside and outside the technology sector are calling for legislators to adopt a similar approach to that of the EU at the federal level.[9]
  - In addition, **responsible and transparent data management by firms can emerge as a source of competitive advantage**. In the end, consumers will be more willing to share their data with companies that are transparent in how they use the data and that make sure data are not accessible to third parties. In this regard, some surveys show that financial institutions enjoy a greater degree of trust among consumers than companies in other sectors when it comes to managing their personal information (see second chart).

Data and trust

Which type of business do you trust the most to securely manage your personal data?
(% of respondents)



Source: *CaixaBank Research, based on data from the Bank of England («The Future of Finance»).*

- **Another equally critical aspect is the responsible application of artificial intelligence techniques to data**. In particular, machines are usually responsible for analysing large amounts of data, using algorithms created by programmers (since we are dealing with many more dimensions than a human mind can conceive). This approach, known as machine learning, allows companies to extract value from data in an automated and scalable manner (for instance, by identifying patterns). However, **the ethical implications of these techniques are complex since, if they are used incorrectly, they can perpetuate biases or prejudices that are present in the data on which these models are based**. As an example, in the application of artificial intelligence techniques to staff selection processes, if the historical data contain an under-representation of women, the algorithm could be biased against this group when searching for candidates. For this reason, it is important to know the biases that exist in the databases that are used, to correct them when designing algorithms that run the machines and to incorporate ethical considerations into the use of such algorithms.

Roser Ferrer

5. See, for example, Lina M. Khan (2016). «Amazon's antitrust paradox». 126 The Yale Law Journal.
6. See, for example, C. Jones and C. Tonetti (2018). «Nonrivalry and the Economics of Data». Stanford GSB and NBER.
7. Bank of England (2019). «Future of Finance».
8. The General Data Protection Regulation (GDPR) sets out how European companies (and global companies that serve the European market) must handle consumer information and determines how to ensure that the consumer gives their consent to the use of those data.
9. In fact, in the state of California, in 2020 an initiative will come into force that is broadly similar to the European GDPR and which has served to launch the debate in the North American country.