


# How can we benefit from Big Data without generating regulatory concerns?

by  **Lucia Batlová**,  
Senior Associate  
Ernst & Young Law  
S.r.o.



**The potential of Big Data is in its capacity to aggregate an enormous amount of information at an incredible speed, and to convey knowledge to predict social behavior, increase security and improve industrial performance. Big Data impacts every field, from intelligent transportation, smart cities, smart manufacturing, to smart health solutions and resource efficiency.**

Organizations using Big Data face many serious legal concerns, such as data handling issues and technical challenges related to architecture, technology, storage, or data analysis. Are entrepreneurs prepared for the legal challenges that accompany Big Data?

## Who owns the Big Data and how can companies protect it?

Some of the data produced in the digital economy may be protected by standard intellectual property laws, for example, the law of copyright. However, an enormous amount of key data for analytics is machine-generated by sources such as sensors and tracking tools on the internet. As such, because it is not protected by exclusive property rights, companies hold and use this data, whilst having no real legal ownership of it. Therefore, the questions of whether knowledge extracted from Big Data may be legally protected and how this can be achieved, are the subject of fierce debate.

The regime, on which companies may rely to some extent, is trade secret protection.<sup>1</sup> In simple terms, a trade secret may include information of commercial value, which has not been publicly disclosed by its holder and which the entrepreneur concerned takes reasonable steps to protect. This means that it is not sufficient for the data to have commercial value; entrepreneurs need also to strive to ensure that their data will not lose its future economic potential, for instance through public disclosure. The commercial value of data may consist in its specific

technical, scientific or business potential and the fact that it is unknown to other entrepreneurs, thus providing a competitive advantage.

The selection of measures which can be considered reasonable for protection of Big Data is by no means straightforward and the type and content of Big Data varies by industry. For example, the most technologically advanced companies, such as banks, telecom providers or automotive producers, usually perform in-house data analytics, while many undertakings use external service providers and tools. The nature of the data is also different. Whereby in marketing management it usually concerns age, gender, nationality, movements of customers within stores or personal preferences, smart devices usually analyze data collected through sensors. This helps to improve performance, safety and predict a breakthrough. It is worth emphasizing that the growth in use of various technologies increases the possibility of theft and espionage of undisclosed information. In this respect, it is advisable for entrepreneurs to implement adequate physical as well as digital measures. These may concern limited access to premises, labeling documents as confidential, implementing solid password protection, encryption, pseudonymization and other protection measures. Non-disclosure agreements with employees, business partners, cloud-service providers and analysts are also a market standard.

## Data privacy concerns: user-friendly consent

Big Data analytics and the digital economy go hand-in-hand with data privacy concerns. A lot of online platforms develop applications that run on users' smart devices, such as mobiles, tablets and smart watches (the so-called Internet of Things). Considering that connected devices are generally produced by a range of different manufacturers, each of them may engage in multiple autonomous data processing activities. As such, the allocation of responsibility between several stakeholders (data controllers or data processors) is much more difficult. This may impact users for instance when exercising their right to object to processing of their data or their right to erasure. Users often complain that the lengthy privacy policies of service providers are written "from lawyers to lawyers". They feel they do not have any option other than to agree if they want to access the service. However, a freely-given consent should not induce purely lengthy formal affirmations. Instead, it should represent a clear, unambiguous, and free choice based on a clear understanding of what will be done with the user's personal data. For instance, a mere ticking of a box without genuine understanding of its consequences would not constitute a valid consent. Also, signing general terms is not sufficient to represent specific consent. Users should always have a further choice to opt out and, if entrepreneurs change their privacy or traffic management policies, users should be immediately informed.

The subsequent use of data presents other issues. Modern data analysis techniques may lend the data to additional uses, which may not always be related to the initial purpose. Seemingly insignificant data collected through a smart device or through the internet can be used to infer information with a totally different meaning. These activities may also relate to persons who are neither subscribers nor users of the respective technology or online tool. In this respect, the service provider should always assess whether the subsequent activities are compatible with the initial declared use.

## How can we get the most out of Big Data?

Companies should not only be able to identify the potential of the data they collect, but also to extract value from it. It is also crucial to ensure that the data will not lose its value over time. Therefore, before any new application or tool is launched, entrepreneurs should seek appropriate tailored measures to protect the data it contains. Only when such measures are adopted, the data may retain its full economic potential. Furthermore, organizations should search for more rigorous and effective methods to mitigate the risks related to Big Data and an effective analytics governance structure must stand as a supporting pillar in the construction of modern risk management.

<sup>1</sup> The European framework represents the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure