

Book Review: Datanomics

Llaneza, P. (2019). *Datanomics*. Barcelona: Ediciones Deusto.
ISBN 978-84-234-3020-8

Patricia Vargas Portillo

Senior Lecturer. ESIC Business & Marketing School. Spain.

ORCID: [0000-0002-0226-3053](https://orcid.org/0000-0002-0226-3053).

jennypatricia.vargas@esic.edu

There is little doubt that Internet is playing an increasingly greater role in our lives and daily tasks. From the moment we get up until we go to bed, we have involuntarily allowed numerous applications to gain access to an extraordinarily large amount of our personal data. It seems unlikely that this trend will reverse itself, and it is quite likely to increase. Our privacy is exposed to the processing of our data without our consent, data violations and even virtual fraud. It should be noted that the latter includes identity theft. There are numerous companies that are working with very sensitive data and that are processing our data in unauthorized ways. Moreover, some of them are increasingly becoming the target of cyber criminals. In this sense, we must allude to a phrase that has been heard for some time now with regard to this particular issue. Data are this century's new black gold. This statement is correct. Even though legislators try to protect user's privacy in various ways, their success is limited. The situation is very complex, as we will see below. It is difficult to place limits on the sea or gates on the countryside.

If we try to place a value on quantitative data, the truth is simply incredible. The fact is that every minute, half a million tweets are sent, more than 60,000 photographs are edited on popular social networks like Instagram, and over three million searches are conducted on the famous Google search engine. These data will probably be exceeded by far in a very short time. As the author rightly states, most of the time when we use the Internet, we accept the terms and conditions, privacy policies and data processing automatically, without even reading them. Ironically, it is very common on a social level to ignore the consequences of what they state. It is difficult, even extremely unusual, to find a user who reads the privacy policy or the general conditions for any data processing they are about to accept. All of this might very soon be something of the past. There are some very interesting projects in Artificial Intelligence that read the privacy policies for us and tell us of any risks that they might pose. Among others, we are referring to Guard. As a matter of fact, the developer of the application has analyzed the privacy policies of some well-known websites such as Netflix, LinkedIn and YouTube, among others. The system determines how many black spots each site has with a very high level of reliability. It is important to emphasize that the results also provide information about cases in which these companies have violated the users' privacy.

More often than we would like, privacy-related problems can be prevented by the users themselves. Among the actions that they can take in this regard, we can mention periodically changing passwords and installing antivirus software. However, there is a certain laziness or reluctance to change passwords. A specific term has been coined to describe this situation. It has been referred to as privacy fatigue.

The book being reviewed is divided into sixteen large sections. It is a work with an extremely interesting and updated content that addresses some very timely issues. The usefulness of the contents is evident. The case study, as is evident in the synopsis, is dedicated to analyzing “all the personal data you give without realizing it and everything that companies do with them.” The laws that protect the users’ privacy are very relevant, as LLANEZA emphasizes with regard to the words of Apple CEO Tim Cook. He refers to the need to have a Federal Privacy Law in the United States. As the author correctly surmises, we have transitioned from a productive economy to a data economy. This statement is quite right.

In line with what was outlined earlier, it is very appropriate to bring up at this time the author’s observations with regard to the privacy paradox. This latter term refers to the fact that while most people seem to show a theoretical interest in their privacy and maintain a positive attitude towards privacy protection, this seldom translates into any real preventive behavior. Many times we share our privacy in exchange for personalized services. On a similar note, not everything on the Internet is free - far from it. Everything has a price. In this case, it is our data. We must be consistent in order to mitigate all the risks that are entailed by our actions. As the author states, “we are aware of the risks, but we don’t want the party to end.”

The observations made about the Google search engine are especially relevant. The search engine collects and processes massive amounts of user data, with an absolutely marvelous potential. Google has many different applications and services that are constantly evolving, and which go far beyond Chrome, Gmail, Maps or YouTube.

We mustn’t lose sight of fake news and the relevance that this can have. In this sense, we must consider the role this played in the latest U.S. elections in which Trump was elected president. As the author indicates, the Russians used fake accounts and bots to share incendiary messages and to manipulate the social networks. Naturally, data processing and creation of profiles by Cambridge Analytics should not go unnoticed. Some voices are of the opinion that the data obtained by this company were used to condition such important events as the U.S. elections and the Brexit. The observations made by McNamee are especially interesting.

In this area, the Internet of things plays a very significant role. There are very popular devices that process many of our data. The author refers to the cases of Alexa and the popular Roomba vacuum cleaner, among others. The statement LLANEZA makes, paraphrasing GEORGE DYSON, makes a lot of sense: “we are creating systems that go beyond our capacity for control.”

SIRI and the Google voice assistant are other tools that process our personal data. Most people surely do not know that our conversations are being listened to by company technicians (without those affected having given their consent). Alexa also acts in the same way. These devices have an infinite potential. For example, Amazon

has registered a patent based on the analysis of the environment to know whether the user is happy, sick or bored, among other moods.

Geopositioning is another topic subject to examination. Google is not the only one to track our movements and monitor us for different reasons, as there are other applications that do the same thing, such as Signal or Silent Phone.

It is quite likely that in the very near future we will reach what the author refers to as the Internet of emotion. In short, this refers to the fact that mobile devices will very soon pay attention to our mood in real time.

The scenario we have just described is as exciting as it is risky. Of concern are our privacy and the non-consented use of our personal data. This is not a minor issue, given the existence of applications and devices that tend to increase our dependence on them. One example, among many others, is the Amazon Alexa device. It is one of the most popular tools, with a more promising future from Jeff Bezos's company. It is said that the popular assistant will try to anticipate the users' desires. Accordingly, it is assumed that it must have an in-depth knowledge of the tastes and personal data of those who have it in their homes. In conclusion, it can be said that unless we take certain precautions, and if we continue to allow companies to manage our data as they like, we will weaken ourselves as people. This can all be compared to what Orwell said. As any seasoned reader will remember, his novel tells about a State that controlled every moment of the lives of its citizens, thus repressing their rights. Information is power, but it is within our right to provide (or not) data about our private lives that can be used against us, through policies aimed at prevention. ▢