

# New coordinates regarding the Internet of Things

**Patricia Vargas Portillo**

Senior Lecturer. ESIC University. ESIC Business & Marketing School. Spain. ORCID: [0000-0002-0226-3053](https://orcid.org/0000-0002-0226-3053).

[jennypatricia.vargas@esic.edu](mailto:jennypatricia.vargas@esic.edu)

Received: June 3, 2021

Accepted: December 4, 2021

Published: May 1, 2022

## Abstract

This article presents a brief theoretical examination of the Internet of Things phenomenon and its promising future prospects.

## Key words

Consumer; Internet of Things; future; business; advertising.

## How to cite this article

Vargas Portillo, P. (2022). New coordinates regarding the Internet of Things. *UNIE Business Research*, XI(1), 41-44. <https://doi.org/10.48132/uniebr.379>.

## 1. New coordinates regarding the Internet of Things

The Internet of Things (IoT) may seem like a phenomenon out of a science fiction movie. However, it is a reality that is widespread in the everyday world (Razzak, 2012). Turning on television with the help of a virtual assistant or changing music with a simple request are some of the tasks that can be performed in a smart home (Srinivasan et al., 2019). With each passing day, the number of activities that the IoT is involved with multiplies, without a limit in sight. In 2020, it was estimated that there were 31,000 million devices in operation that could be included in the IoT.

Next, we explore some types of connected objects that can be found today. In most cases, these objects are invisible to people (Gigli & Koo, 2011). We all have at home, without being aware, a number of devices that meet the definition. As the implementation of 5G technology advances, the IoT will have, if possible, an even more important role. It is a key concept for improving the quality of life of people and offering increasingly better services (Butler, 2006).

Everything we analyze is related to the digital interconnection of the objects we use in our daily lives (López Jiménez, Dittmar & Vargas Portillo, 2021a). The term IoT was used, for the first time, by Kevin Ashton at the MIT Auto-ID Center. He stated that if, for example, all devices were connected to the internet and had identification sensors, there would be no problems related to the expiration date of medicines or food. Kevin Ashton used the expression publicly in an event that generated great excitement. However, we must go back to 1990 to see the first IoT gadget in history, when John Romkey presented a toaster that could be remotely turned on and off.

The IoT offers a series of unquestionable benefits on a day-to-day basis. Among them, we highlight the following: the possibility of connecting a computer to the internet and enjoying all the associated advantages; greater speed in the exchange of information; better decision-making; more automation; and energy savings.

The economic factors must also be taken into consideration. By using less energy, we pay less. The devices are also able to alert us to possible failures so that we can attend to these issues before they become serious. Any device that can connect to the internet through a network or, failing that, to another device through Bluetooth that offers this type of connectivity is considered to belong to the IoT (López Jiménez, Vargas Portillo & Dittmar, 2022a).

When IoT devices take the form of accessories that we can wear, they are called wearables. Through small devices with integrated sensors, it is possible to collect data. That information is sent to smartphones. The most relevant applications of wearables can be found in sports and, more specifically, in some clothing items.

Health control is one of the aspects in which the IoT is most useful. In this sense, we can highlight the smart scales that are capable of providing a multitude of data. Within the latter, we can, as an example, indicate the percentage of body fat, bone mass, water, or metabolic age. There are various devices with which medical professionals can observe the vital signs of patients without having to go through a consultation, known as real-time health systems.

Likewise, this technology has allowed us to cook in a healthier and simpler way, as demonstrated by connected oil-free air fryers. To date, there are smart coffee makers, fryers, and even pressure cookers that make cooking easier.

The IoT has also reached the universe of light switches. This allows one, through a mobile phone or a virtual assistant, to turn the lights on and off, change their color, and regulate the light intensity. The IoT is also present in garbage cans. This signals when the bag is full to automatically seal it and replace it, all by virtue of sensors.

Another essential element for enjoying a connected home is a smart refrigerator. Moreover, smart thermostats can activate a home heating or air conditioning system if the temperature drops below or exceeds a predetermined value (the comfort temperature). Undoubtedly, this is an ideal way to save energy, protect the environment, and spend less.

The world of connected devices has moved from the home to the garden with intelligent systems that take care of the lawn at different levels: cutting, watering, and monitoring, all automatically, remotely, and planned.

The automotive industry has focused on developing safer and more efficient cars, but in recent years, attention has also been focused on improving the experience of users inside the vehicle. All the major brands in the sector, globally, have connected car systems, which not only allow relation to other objects but also turn the car into a mobile IoT device.

IoT technology has reached physical stores, making work easier and the customer more satisfied. The main novelty is the introduction of sensors in all types of common elements in a store with the mission of studying the behavior of buyers. There is a wide range of situations in which the IoT can intervene within a supermarket (Nowland, Necka & Cacioppo, 2018).

However, although the IoT has numerous advantages, it also has potential disadvantages. Hackers have specialized knowledge about attacking these devices to access their data or industrial control systems. There are countless sensors and IoT computing devices that are connected to a large part of the global infrastructure (López Jiménez, Dittmar & Vargas Portillo, 2022b). Most of these devices were designed before hackers and electronic intrusions entered our consciousness. Now, the security and privacy of the IoT must be the most important factor (López Jiménez, Dittmar & Vargas Portillo, 2021b).

The Cambridge Analytica scandal highlighted the danger of mass collection and use in manipulating the decisions of its holders (Hinds, Williams & Joinson, 2020). The company used data obtained from different sources, including those of millions of Facebook users, to, among other things, employ targeted advertising and thereby influence the United States elections and change the direction of the vote for the separation of the United Kingdom from the European Union. It obtained the data, fraudulently, through this social platform where users interact and voluntarily share personal information. We must be fully aware that the information in our home is managed by the companies that provide the devices we use. We should not think that we are buying a smart watch but that we are hiring the service of someone to monitor our behavior. It is necessary to establish security measures that, due to the large amount of data that these devices can store and

because of how compromised the information can be, prevent unauthorized access and guarantee the confidentiality, integrity, and availability of the data.

There is no going back. We now live in an interconnected world. Around us, there is a huge number of devices that communicate with each other, linked by a network of networks. In short, with an internet connection and a mobile phone, we can open garage doors, turn on light bulbs remotely, lower, raise, and close blinds, or carry out any other process in an automated way, as long as we have the appropriate connected device. Although the digital transformation of thousands of companies was exponential during the pandemic, this does not mean that we can forget the negative impacts that this could generate, so proceeding in a conscious way and with friendly technology provides added value to the evolutionary process.

## 2. References

- Butler, D. (2006). 2020 Computing: Everything, Everywhere. *Nature*, 440, 402-405. <http://dx.doi.org/10.1038/440402a>
- Gigli, M., Koo, S. G. M. (2011). Internet of Things, Services and Applications Categorization. *Advances in Internet of Things*, 1(2), 27-31. <https://doi.org/10.4236/ait.2011.12004>
- Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>
- Srinivasan, C. R., Rajesh, B., Saikalyan, P., Premasagar, K., & Sarath Yadav, E. (2019). A review on the different types of internet of things (IoT). *Journal of Advanced Research in Dynamical and Control Systems*, 11(1), 154-158.
- López Jiménez, D., Dittmar, E. C., & Vargas Portillo, J. P. (2022a). Consumer Trust in the Digital Environment: Dispute Prevention and Alternative Dispute Resolution. *Revista de Direito, Estado e Telecomunicações*, 14(1), 113-138. <https://doi.org/10.26512/lstr.v14i1.37820>
- López Jiménez, D., Dittmar, E. C., & Vargas Portillo, J. P. (2022b). The trusted third party or digital notary in Spain: effect on virtual transactions. *International Review of Law, Computers & Technology*, 36(3), 453-469. <https://doi.org/10.1080/13600869.2021.2004760>
- López Jiménez, D., Dittmar, E. C., & Vargas Portillo, J. P. (2021a). Protecting minors in relation to interactive software. *Revista de Direito, Estado e Telecomunicações*, 13(1), 20-39. <https://doi.org/10.26512/lstr.v13i1.29743>
- López Jiménez, D., Vargas Portillo, J. P., & Dittmar, E. C. (2021b). Self-regulation of sustainability as a manifestation of corporate social responsibility. *Revista de Ciencias Sociales*, 27(3), 16-29. <https://doi.org/10.31876/rcs.v27i3.36750>
- Nowland, R., Necka, E. A., & Cacioppo, J. T. (2018). Loneliness and Social Internet Use: Pathways to Reconnection in a Digital World? *Perspectives on Psychological Science*, 13(1), 70-87. <https://doi.org/10.1177/1745691617713052>
- Razzak, F. (2012). Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia Computer Science*, 10, 658-665. <http://dx.doi.org/10.1016/j.procs.2012.06.084>