LUISS

Dipartimento di Economia e Finanza

Corso di laurea in Economics & Business

Cattedra di Principles of Civil Law

Internet of Things: Competitive Features and Concerns

RELATORE

Prof. Avv. Valerio Cosimo Romano

CANDIDATO

Mario Previti Flesca

Matricola 229571

ACADEMIC YEAR 2020-2021

SUMMARY

INTRODUCTION

This thesis deals with the structural difficulties that prevent smart device manufacturers and/or Internet of Things (IoT) service providers from entering/expanding within the IoT market and competing on equal terms with Big Tech giants such as Amazon, Google and Apple.

The reasons that led me to address this topic is my particular interest in the competitive aspects that characterize expanding and developing markets. I therefore decided to examine the IoT market as it has all the requirements that generate particular curiosity in me. In addition, being able to talk about a sector that particularly affects daily life, especially for young people like me, was one more reason that conditioned the choice of the subject.

The primary objective of the thesis is therefore to analyze in depth the competitive characteristics of the IoT market. In this regard, particular reference will be made to the recent preliminary investigation, launched by the European Commission, in which concerns have emerged regarding the enormous competitive advantage that the Big Tech companies have over any other corporation operating in the industry. This unique positioning may allow these giants to condition and direct consumer choices in their favor, discouraging other providers to invest in innovation, maintaining a real oligopoly and a progressive 'race to the bottom' in which the quality of products and services do not guide consumers' purchasing decisions.

Specifically, in the first chapter the technical characteristics of an IoT ecosystem and its main fields of application will be explained. In addition, a brief overview will be given on the main segments of the (IoT) market and on the evolutionary steps that have characterized the industry from its birth to the present day. In the second chapter we will examine the effect that the IoT has in the mankind's daily life and the various related problems associated with the protection of sensitive data. In the third chapter, the characteristics of competition in the IoT sector will be briefly explained. In the fourth and final chapter, instead, all the concerns that the interviewees, the subject of the sector survey carried out by the European Commission, have raised will be highlighted.

Hopefully, at the end of the thesis, the difficulties and obstacles that prevent smaller companies from expanding within the IoT industry will be clear, with the prospect that the Directorate-General for Competition (DG COMP) – "in charge of establishing and implementing competition policy for the European Union" – will take decisions aimed at protecting those realities that do not have many weapons available to make room in the 'Internet of Things' sector.

CHAPTER 1: WHAT IS MEANT BY 'INTERNET OF THINGS' (IoT)

1.1 Definition, evolutionary stages and development expectations

The term 'Internet of Things' indicates that set of technologies that are able to connect any type of equipment to an Internet network. Although the aforementioned term was introduced relatively recently, the concepts to which it refers essentially date back to the second half of the twentieth century with the birth of the internet and the semantic web i.e., a web made up of things and not lines of code.[1]

The concepts underlying the IoT have been developed since 1982, when some researchers of the time of a private Institute in Pittsburgh (Pennsylvania) tried to apply and connect sensors and the internet to a distributor of university drinks, to allow students to check through a code if the drink they wanted to buy was available in the vending machine, without having to go to check in person. Subsequently these concepts will be resumed in 1991 in the article *The computer of the 21st Century* by Mark Weiser (considered a point of reference in the field of information technologies) published in the popular magazine *Scientific American*, but also more decisively by Reza Raji in the IEEE technical magazine in 1994. In particular, Reza Raji in his article *Smart networks for control* explained that connecting to the internet and automating the operation of a wide range of items (from simple household appliances to objects used within firms' production mechanisms) is becoming, with the passage of time and research, an increasingly practicable and concrete practice on which to rely both for the present and for the future. The term 'Internet of Things' was coined a few years later: in 1999, a researcher from MIT (Massachusetts Institute of Technology) and executive director of Auto-ID Center (The leading academic research network on the 'Internet of Things') named Kevin Ashton used it for the first time during a presentation at Procter & Gamble (P&G) in order to draw senior management's attention to a fascinating new technology

[1] M. Bellini, "IoT (Internet of Things): cos'è, come funziona ed esempi" [IoT (Internet of Things): what it is, how it works and examples], in Internet4Things, available at https://www.internet4things.it/iot-library/internet-of-things-gli-ambiti-applicativi-in-italia/ (last visited 4/09/2021).

called RFID (Radio Frequency Identification): An innovative system to facilitate the management of objects through computer.[2]

The use of the 'Internet of Things' formula will be subsequently extended to any object/device capable of using an internet connection to perform a specific action through a particular mechanism, according to which the real world is connected to the virtual world via sensors.[3]

But what does the name 'Internet of Things' really mean? This neologism is often compared to the field of telecommunications. It arises from the need to give a concrete and definitive definition to the connection of real objects to the virtual world of Internet. The main purpose of the IoT is to monitor and allow the transfer of information and data in order to allow objects to perform subsequent logical actions[4]. Let's make some examples: IoT is an internet controlled coffee maker able to be controlled and managed by a downloadable application on your smartphone; IoT is also a wireless home automation system capable of improving efficiency and comfort of a firm, through an integrated function which allows the various company electronic systems to be managed remotely by means of a single device; IoT is also a voice assistant device (e.g., Alexa by Amazon), which, through simple voice commands, is able to perform specific actions such as providing information found from the web through its ability to connect to an internet network.

In the embryonic stage of development, only some devices were capable of collecting data, and only within a limited number of application areas. This working process was made possible by means of sensors of information detection that

[2] K.L. Lueth, "Why the Internet of Things is called Internet of Things: Definition, history, disambiguation", in IOT ANALYTICS, available at https://iot-analytics.com/internet-of-things-definition/ (last visited 4/09/2021); P. Todorovich, "L'Internet delle cose (IoT): cos'è e come rivoluzionerà prodotti e servizi" [Internet of Things (IoT): what it is and how it will revolutionize products and services], in ZeroUno, available at https://www.zerounoweb.it/analytics/big-data/internet-of-things-iot-come-funziona/ (last visited 4/09/2021); "Evolution of Internet of Things (IoT): Past, present and future", in Techahead, available at https://www.techaheadcorp.com/knowledge-center/evolution-of-iot/ (last visited 4/09/2021); K. Ashton, "That 'Internet of Things' Thing", in RFID Journal, available at https://www.rfidjournal.com/that-internet-of-things-thing (last visited 4/09/2021).

[3] *Ibid*.

[4] M. Bellini, *op.cit.*

subsequently allowed its transformation into digital data through manual processes i.e., without the use of an Internet connection. However, after the initial phase of development, the definitive passage from sensors to the IoT took place: an innovation system where the object is connected to an internet network, a sensor detects its data which are then distributed within the network itself. The different stages of progress of the IoT sector and its technological advancement processes can be synthesized as follow: (i) Wireless devices capable of detecting and communicating digital data; (ii) Wireless devices capable of detecting and transferring a broader spectrum of types of digital data; (iii) Wireless devices capable of elaborating a process of selection of data to be transferred which are able to obtain very specific requirements; (iv) Wireless devices capable of carrying out a database collection of selected data that allow the device to perform an indicated action; (v) Wireless devices capable of detecting, selecting, and transmitting only the relevant data capable of allowing the device to operate an action response.[5]

In recent years, the 'Internet of Things' area has registered a dramatic increase in terms of number of connected IoT devices, allowing for the wide-ranging development of countless fields of application and sectors: today, the estimated number of IoT devices connected to the internet is around 7 billion, extending from security systems to the improvement of the environment, from urban development to the world of biotechnologies, allowing us to satisfy many desires, needs and problems that are still unsolved nowadays[6].

The rapid expansion of the IoT can be substantially traced back to the technological developments occurred during the last decade in the fields of electronics and wireless communication (e.g., creation of microscopic-scale sensors such as micro-electromechanical systems and Micro Electro-Mechanical Systems), as well as the rapid spread of digitization globally. A decisive role was also played by the proliferation of Wi-Fi networks and the development of the Bluetooth technology, both of considerable

[5] *Ibid*.

[6] "IoT: What to expect in the future", in Green volcano technologies, https://www.greenvulcano.com/iot-what-to-expect-in-the-future/ (last visited 4/09/2021).

importance for managing problems such as distance, energy limitations and the huge amount of data to be transferred[7].

The evolution path of the IoT sector seems destined to continue smoothly at full speed, both in the short and long run: technological progress will bring improvements that in particular will concern an increased network agility, the integration of artificial intelligence (AI) within already advanced wireless devices, and the ability to automate and distribute data collection in order to produce more quality software and devices on a global scale. In this regard, Gartner, a leading research and advisory company, predicts that by the end of 2021 there will be approximately 25 billion connected devices[8]. Furthermore, other industry experts claim that the threshold of 75 billion IoT devices will be exceeded by 2025. To conclude, although no certain predictions can be made, what is evident is that the IoT industry will continue to grow exponentially over the next few years, leaving an increasingly indelible mark on our lives and habits[9].

1.2 Fields of application and characteristics of an IoT infrastructure

The recent years remarkable expansion of IoT technology is allowing it to find space in multiple fields of application. In fact, the IoT is an advanced technology that has the advantage of being able to be applied in any sector, capable of providing increasingly cutting-edge performance over time. However, although the IoT technology tries to find always more innovative ways of development, it does not always find exploitable fertile ground: the effectiveness with which the IoT manages to develop within a given sector largely depends on the available supporting technologies, on the interest present in that specific development area, and on the value that the creation of a particular intelligent object brings to the user.[10]

[7] "Con l'Internet of Things il mondo diventa smart" [With the Internet of Things the world becomes smart], in ItManager.space, available at https://itmanager.space/internet-of-things/ (last visited 4/09/2021).

[8] "Future IoT", in Ericsson.com, available at https://www.ericsson.com/en/future-technologies/future-iot (last visited 4/09/2021); Green volcano technologies, *op.cit.*

[9] "The Rise of IoT: The History of the Internet of Things", in Simon IoT, available at https://www.simoniot.com/history-of-iot/ (last visited 4/09/2021).

[10] Revel Gian Marco, "Introduzione al mondo dell'Internet of Things" [Introduction to the Internet of Things world], in Ingenio, available at https://www.ingenio-web.it/23301-introduzione-al-mondo-dellinternet-of-things (last visited 4/09/2021); ItManager.space, *op.cit.*

Among the sectors within which the IoT recorded the greatest growth and development margins, is the industrial one. In fact, according to some collected data, about 97% of companies have introduced IoT systems within their industrial processes, favouring their automation and greater safety and efficiency. Therefore, it can be said that, over the years, this area has undergone the strong influence of the digital progress, gradually giving life to a more *avant-garde* parallel sector: the 'Industrial Internet of Things' (IIOT). The IIOT operates exclusively within industry 4.0, integrating new technologies that aim at the optimization of production processes, including the connection of several elements at the same time allowing to work with a greater amount of information, new production technologies aimed at improving working conditions, and specific devices allowing to work in harsh industrial environments improving the production quality of existing plants.[11]

Specifically, today we talk about IoT applied to the industry sector in the areas of production, logistics and the process of creating new products to be launched on the market. In particular of:

- Smart factory, which concerns the control of production processes and quality, the maintenance, and the management of workplace safety and industrial waste.
- Smart lifecycle, which concerns the process of creating new products, including the management of suppliers in the embryonic phase, and the strategic management of the end of the life of a product.
- Smart logistic: which concerns the industrial tracking and monitoring through RFID technology, as well as security in the most complex logistics centres.[12]

Another sector in which the IoT has found fertile ground, recording strong growth and expansion, is that of Safety & Security. The need for technological intervention in this sector was evident, and the IoT has contributed to making the supervisory elements capable of connecting and communicating with each other, making their performance to improve.[13]

Other sectors that are adopting IoT solutions are those that concern health (e.g., the development of devices that can remotely monitor the conditions of patients) and

[11] *Ibid*.
[12] *Ibid*.
[13] *Ibid*.

construction. The latter can now be referred to as "IOT Buildings", thanks to the introduction of new mechanisms which make this sector more technologically advanced than others. This term refers to objects communicating with each other via an internet network allowing to improve both the control and effectiveness in building management and the user experience. However, the fields of application of this technology within the building sector are many, some examples of which are: smart mobility, smart cities and smart homes.[14]

Specifically, smart cities are cities equipped with innovative technologies applied to the urban framework, and the objective of the IoT technology within this specific branch of application does not only concern the improvement of people safeness inside individual buildings, but also the improvement of the level of comfort and sustainability within cities as a whole: typical examples are smart cameras, capable of identifying faces and objects, intelligent microphones, capable of detecting road accidents in real time to be immediately reported to emergency response patrols, automatic irrigation plans for parks based on temperature levels, or systems that allow for the coordination of traffic lights in the event of public or health emergencies.[15]

Smart homes, on the other hand, are homes connected to the internet that can guarantee energy savings (and savings on the bill), well-being and safety through systems allowing an internal remote management. An illustrative example is the intelligent voice assistant, capable of performing numerous functions via simple voice commands.[16]

As for smart mobility, it is about intelligent vehicles designed to prevent road accidents and reduce fuel consumption, thanks to an innovative system capable of connecting with other vehicles, regulating cruising speed and promptly reacting to surrounding movements.[17]

1.3 Characteristics of an IoT infrastructure

Although the Internet of Things can be applied in a variety of very different areas, its structure has recurring components. In particular, there are 5 key elements through which data flow within a network for analysis and processing: sensors and actuators (i.e.

[14] *Ibid.*
[15] *Ibid.*
[16] *Ibid.*
[17] *Ibid.*

system terminals), which have the task of observing various parameters (e.g., temperature) or perform actions on demand. The network (i.e. the networked computer structure), which performs the function of processing and transmitting data. The cloud, which has the fundamental role of hosting and protecting the data regularly transferred from the network. The analytical component, which has the task of carrying out the analysis, evaluation and decision processes (it is located within the cloud and represents the core of the IoT infrastructure). Finally, the user interface, which is an intuitive interface that allows the interaction between the device and the end user, the only one able to make informed decisions based on their needs.[18]

1.4 Main consumer IoT segments

The main segments of the consumer IoT industry are: voice assistants, smart home devices, wearable devices and consumer IoT services. In this section we will discuss about their characteristics and the mechanisms through which the interaction with the user takes place.

With regard to voice assistants, they can be defined as software that can be activated through simple voice commands, capable of performing a wide range of actions on instruction by the user. In particular, there are mainly two types of voice assistants: generic ones and specialized ones. Generic voice assistants are so named for the numerous functions and activities they are able to perform, such as playing music, accessing information via web, automatically managing domestic heating systems (and more), planning daily activities etc. Typical examples of generic voice assistants are Apple's Siri (launched in Europe in 2011), Amazon's Alexa and Google's Google Assistant (2016), and finally Samsung's Bixby (2018). Currently, the most prominent and most used voice assistants within the Consumer IoT sector on the European continent are Google Assistant and Alexa. Specialized voice assistants, on the other hand, are so called due to their limitation in the built-in features they are able to perform. In fact, they are usually suited

[18] *Ibid.*; A. Jahnke, "The 4 Stages of IoT Architecture", in Digi, available at https://www.digi.com/blog/post/the-4-stages-of-iot-architecture (last visited 4/09/2021); "Network", in Wikipedia, The Free Encyclopedia, available at https://it.wikipedia.org/wiki/Network (last visited 4/09/2021); "User interface", in Wikipedia, The Free Encyclopedia, available at https://en.wikipedia.org/w/index.php?title=User_interface&oldid=1031291510 (last visited 4/09/2021).

to carry out a limited number of activities circumscribed to the services that the device, to which the voice assistant refers, is qualified to provide (e.g., Cortana by Microsoft). Also, unlike generic voice assistants, which are available in most of the world's languages, specialized voice assistants are only available in a limited number of languages (usually one or two).[19]

The stages through which the interaction between voice assistants and users occurs can be synthesized as follow : (1) the device activation through a keyword e.g., ‘Hey Siri’ (on some devices you must first press a power button); (2) the voice command e.g., ‘turn on the heating’; (3) the voice assistant’s processing of the user's request; (4) the answer from the voice assistant.[20]

As for smart home devices, they represent a niche within the home IoT industry that encompasses a wide range of devices, which can be categorized as follow: smart home entertainment devices (e.g. smart TVs), home security devices (e.g. smart security cameras), comfort devices (e.g. smart air conditioners), and smart home appliances (e.g. robot vacuum cleaner).[21]

The interaction between the smart home device and the user takes place through the user registration on a smart home application of the device manufacturer (usually downloadable via smartphone through the stores of the main operating systems, or via computer). Consequently, this will allow the user to remotely configure and manage the connected device via a very intuitive user interface. Although most domestic environment IoT devices can only be managed from the manufacturer-provided user interface, more and more companies are progressively authorizing third-party manufacturers to produce their own one, so to improve the consumer experience by promoting the interoperability of heterogeneous environments with multiple brands.[22]

As for wearables, they are devices equipped with sensors that can transmit and collect data over an internet network, powered by an operating system. Some examples of wearable devices are smartwatches, augmented reality headsets, and smart glasses.

[19] European Commission, “*Preliminary report – Sector inquiry into consumer Internet of Things*”, available at https://ec.europa.eu/competition-policy/system/files/202106/internet_of_things_preliminary_report.pdf, 2021, p.20
[20] *Id.*, p.21
[21] *Id.*, p.22
[22] *Id.*, p.22-23

Their limitation is to have a reduced data storage and processing capacity, making it essential to use them via smart mobile devices through complementary applications that can be managed directly from the user's smartphone. This way, while some notifications can only be viewed on the wearable device display, others can only be viewed via the companion app on the smart mobile device.[23]

The last consumer IoT segment concerns consumer IoT services, which refer to a large number of services (e.g. security, lighting, health, information services, etc.) usable both through user interfaces of smart devices, and from smart computers or mobile devices. Currently, most IoT services are accessible from smart devices via the Android and Apple operating systems, as well as from third-party voice assistants such as Google Assistant and Alexa. However, consumer IoT is trying to progressively introduce alternative access routes (e.g. via voice commands), working on the involvement and interoperability of heterogeneous smart devices and services. Furthermore, according to data collected by the European Commission, about half of consumer IoT services require user registration as a prerequisite for use and, in some cases, a minimum age requirement. In addition, some services require a subscription, such as premium services with limited public access.[24]

[23] *Id.*, p.23-24; "Consumer Internet of Things (CIoT) – what is it and how does it evolve?" in I-Scoop, available at https://www.i-scoop.eu/internet-of-things-guide/what-is-consumer-internet-of-things-ciot/, (last visited 4/09/2021).

[24] *Id.*, p.24-25

CHAPTER 2: CONSUMER INTERNET OF THINGS ENVIRONMENT

2.1 How Internet of Things is shaping consumer behaviour

The creation of new data sources, facilitated by the interaction and interoperability of IoT devices, is allowing companies to optimize customer activation and loyalty processes through personalized content that increasingly meets the needs of the customers they are targeting. An effective strategy in this sense guarantees companies a credible positioning within the market in which they operate, and a trend towards success in line with their objectives. The role of the IoT technology, however, does not stop at this: IoT not only allows the development of effective strategies in line with the objectives of a company but, in combination with data analysis and behavioural science, it also represents a powerful persuasive tool capable of altering consumer behaviour.[25]

Technological development, combined with the discipline of data analysis and behavioural sciences, is giving rise to increasingly automated and cutting-edge mechanisms regarding the analysis of consumer behaviour, allowing the development of extremely valid strategies for the sale of products and services, and also facilitating the work of behavioural specialists and allowing the optimization of the performance quality within the marketing and economic sectors.[26]

The abundant amount of data produced by consumers through the use of their IoT devices, which are subsequently transferred to the databases of the companies they interact with, allow the latter to make optimal decisions on the type of ad and on the type of communication they want to adopt to induce consumers to take a certain action. To date, about 1 billion gigabytes of data per month are produced only by smartphones and, over the years, the number of objects that will have the capacity to collect data will certainly increase. Indeed, as we have seen in the previous chapter, IoT technology is entering our cities, our homes and even our clothes: this transition from the world of the 'Internet of People' (IoP) to that of the 'Internet of Things' (IoT) is allowing us to expand

[25] B. Nunes & D. Goncalves, "Three ways the Internet of Things Is Shaping Consumer Behavior", in begavioraleconomics.com, available at https://www.behavioraleconomics.com/three-ways-the-internet-of-things-is-shaping-consumer-behavior/, (last visited 4/09/2021).

[26] *Ibid*.

the marketing strategies that influence human behavioural and decision-making neuronal processes in the world of purchases in an increasingly incisive way.[27]

IoT technology is shaping consumer behaviour in three different ways:

(i) it represents a valid new data source for machine learning algorithms.

Most of the algorithms for machine learning use the technique of *predictive modelling* i.e., "*the salient phase of predictive analysis that includes methodologies and techniques capable of extracting knowledge from available data to make predictions on data or events in the future*".[28] An example of this are *activity trackers* i.e., devices capable of measuring heart rate, sleep quality, and other similar fitness metrics: these types of devices are based on machine learning algorithms powered by resources present in the cloud, which allow us to establish our real health condition and, based on it, determine when we need a medical intervention. Other more sophisticated devices are even able to monitor the level of various blood parameters, and to send a warning to the user suggesting him to take a certain drug or a certain amount of food containing the right macronutrients necessary to restore health. In sight of this, we can say that data from IoT devices allow us to predict certain actions through metrics strictly related to induced behavioural aspects.[29]

Another case of machine learning, used as a tool for persuasion and conditioning of consumer behaviour, concerns the dynamic offer of products and services in the tourism sector. A clear example of this are travel service provider websites such as *Booking.com*, *Expedia*, and *Airbnb* that provide personalized suggestion systems based on socio-demographic data and previous user behaviour. Furthermore, in recent years these companies have expanded their services by implementing smartphone applications aimed at simplifying the accommodation booking process.

In addition, recently, Booking.com has extended its services with the launch of a new product: Booking Experiences i.e., a service that uses artificial intelligence and machine learning to predict and meet the needs of traveling tourists, creating personalized

[27] *Ibid*.

[28] Redazione Osseratori Digital Innovation, "Che cos'è la Modellazione Predittiva e come funziona" [What Predictive Modeling is and How it Works], in osservatori.net digital innovation, available at https://blog.osservatori.net/it_it/modellazione-predittiva-come-funziona, (last visited 4/09/2021).

[29] B. Nunes & D. Goncalves, *op.cit.*

activity proposals. With this product, booking is definitively eliminating, for the user, the need to book in advance or to queue for the purchase of entrance tickets for the main tourist attractions, thus simplifying and optimizing the experience of individual travellers: they just need to scan the QR code provided at the entrance of the attraction, linked to the credit card of the selected user, to access it.

(ii) it adds value to the consumer during the pre-sale and after-sale periods.

In any sector, the set of business processes are made up of activities that aim to bring value both to companies and consumers, during the pre and post-sales phases. During the first phase, the IoT technology allows the company to optimize earnings and to customize the offer according to the type of customer it is dealing with. An example of an IoT ecosystem, created by the interaction between two separate digital environments to acquire behavioural data, is Admiral's *FirstCarQuote* i.e., a service offered to insurance companies to help them solve the problem of information asymmetry that has always plagued them: through their service they help insurance companies to distinguish a reliable novice driver from one who is less so, given the lack of his (or her) historical driving record. In fact, shortly before the underwriting phase of the insurance policy, the website requires the young potential buyer to log in to his Facebook profile which, through an artificial intelligence algorithm, scans his actions performed in the past on the social network platform, and subsequently measures the probability that the person may cause a road accident, basing the outcome on pre-established behavioural parameters.

This technological orientation aimed at perfecting the behaviour analysis has positive implications also for what concerns the phase following the sale of a product/service. An example, still remaining in the auto insurance sector, concerns the possibility for insurance companies to send personalized quotes to encourage their customers to behave more prudent and responsible when driving. A similar example can also be found in the banking sector with HBSC i.e., a European credit institution that monitors its customers' expenses, helping them to achieve long-term financial goals by sending regular messages aimed at stimulating the ethics of savings.[30]

[30] *Ibid.*

(iii) it provides improved causal inference methods by facilitating the processes of generalization of the obtained results.

To test the effectiveness of a specific treatment aimed at a specific audience segment, and subsequently evaluate the intensity of a possible consequent change in its behaviour, behavioural scientists exploit data coming from randomized control trials (RCTs), which occur through a random subdivision of the target audience into separate groups, to which different selected treatments are applied.[31] Similarly, digital marketing experts use the A/B testing function present in the main digital platforms for advertising campaigns (e.g., Facebook) to test the effectiveness of slightly different ads offered to different segments of the same target audience. Both methods of analysis are based on the principle according to which correlation does not imply causation. Therefore, given the amount of data and information that IoT devices are able to generate with respect to individual preferences and tastes, this sector covers a fundamental role in the personalization of treatments, which is a key factor in optimizing their performance and in perfecting causal inference methods.[32]

To conclude, the IoT technological development, associated with the discipline of data analysis and the science of behaviour, are giving us the possibility to achieve experimental results never achieved before within the DIKW hierarchical model (data, information, knowledge and wisdom).[33] In fact, while data analysis allows us to extract useful information from raw and incomplete data, and behavioural science allows us to gain awareness of the acquired data and subsequently to give it a contextualized empirical value, personalized data from the IoT world allow us to convert the extrapolated data into thoughtful behavioural predictions.

2.2 The market of IoT and its growing opportunities

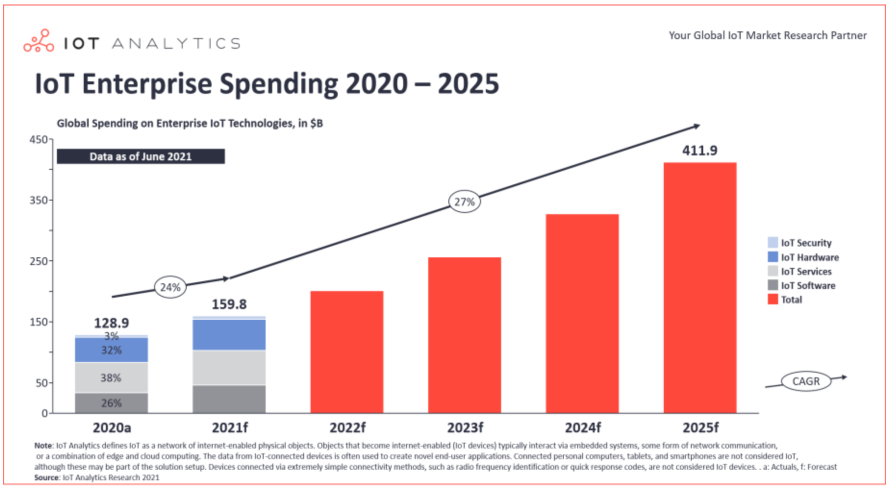
The exponential growth of IoT technology in recent years, combined with a constant increase in the number of devices capable of connecting to an internet network,

[31] "Studio controllato randomizzato" [Randomized controlled study], in AGINGPROJECT, available at https://www.agingproject.uniupo.it/glossario/studio-randomizzato-controllato/ (last visited 4/09/2021).

[32] B. Nunes and D. Goncalves, *op.cit.*

[33] "What is the Data, Information, Knowledge, Wisdom (DIKW) Pyramid?", in Ontotext, available at https://www.ontotext.com/knowledgehub/fundamentals/dikw-pyramid/ (last visited 4/09/2021).

has encouraged companies to increase their investments in a sector in such rapid expansion and with ample room for improvement and strengthening. To date, according to *IoT Analytics*, global investments by companies in the IoT industry are estimated to increase, from $ 128.9 billion in 2020, to approximately $ 159.8 billion by the end of 2021 (increase of 24%). Moreover, in the years to come, corporate spending on IoT is expected to increase by 26.7% annually, reaching $ 411.9 billion by 2025. (Next Figure).[34]

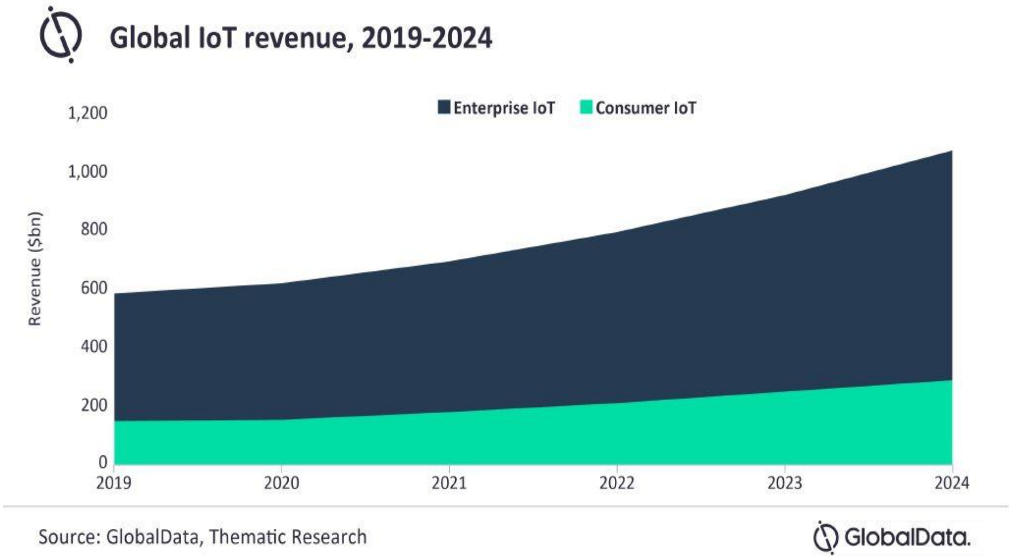

IoT Enterprise Spending 2020 – 2025

Global Spending on Enterprise IoT Technologies, in $B

Note: IoT Analytics defines IoT as a network of internet-enabled physical objects. Objects that become internet-enabled (IoT devices) typically interact via embedded systems, some form of network communication, or a combination of edge and cloud computing. The data from IoT-connected devices is often used to create novel end-user applications. Connected personal computers, tablets, and smartphones are not considered IoT, although these may be part of the solution setup. Devices connected via extremely simple connectivity methods, such as radio frequency identification or quick response codes, are not considered IoT devices. . a: Actuals, f: Forecast
Source: IoT Analytics Research 2021

Additionally, the size of the global IoT market, from GlobalData's estimated $622 billion revenue in 2020, is expected to reach $1 trillion by 2024, with a compound annual growth rate (CAGR) of around 13%. (Next figure).[35]

[34] P. Wegner, "Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security", in IOT ANALYTICS, available at https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/ (last visited 4/09/2021).
[35] GlobalData, "Global IoT Market to Surpass $1 Trillion Mark by 2024", in EET ASIA, available at https://www.eetasia.com/global-iot-market-to-surpass-1-trillion-mark-by-2024/ (last visited 4/09/2021).



Global IoT revenue, 2019-2024

Source: GlobalData, Thematic Research

The growth of the 'Internet of Things' market is stimulated by the constant progress and development of sensor technology integrated into the IoT devices (crucial for the functioning of the data collection and demand distribution process), and by the ever increasing demand for devices equipped with IoT technology by multinationals and companies operating in every field of work and related to every part of the globe, as it is able to improve productivity and optimize the personalization of content to offer to customers.[36] In fact, according to some data collected, "*The number of companies using IoT solutions has increased from 13% in 2014 to about 25% today, and the worldwide number of connected devices is expected to increase to 43 billion by 2023 (a nearly three-fold increase from 2018)*".[37] In addition, the progress of this technology is gradually allowing manufacturing companies to increasingly simplify some mechanisms of use, and to lower the production costs, of its components, making them cheaper and facilitating their application within the business context. All this, inevitably, is bringing benefits to small and medium-sized enterprises that have the opportunity to break down some entry barriers of a sector, that of the IoT, dominated (until now) by large companies.[38]

Other factors that are driving the growth of the global IoT market relate to the need for companies to keep pace with technological advancement. But above all they

[36] F. Dahlqvist, M. Patel, A. Rajko, and J. Shulman, "Growing opportunities in the Internet of Things", in McKinsey & Company, available at https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things (last visited 4/09/2021).
[37] *Ibid*.
[38] *Ibid*.

relate to the opportunity to have a competitive advantage over the competition, by exploiting the IoT through the implementation of differentiation strategies, and through the implementation of unique, improved and optimized services to be offered to consumers.[39] In this sense, the North American market appears to have accelerated operations by increasing its share of investments in this sector: it is expected that, within the next two years, it will come to hold the largest market share of the entire IoT industry. In particular, in recent years, the United States and Canada have been exponentially increasing their investments in research and development (R&D) activities within industry 4.0, with the aim of increasing their competitiveness by exploiting the IoT for the management and the optimization of company production processes.[40] To date, the companies that control the largest cash flows, and which hold the most value in terms of equity capitalization within the 'Internet of Things' market, are American companies such as Verizon ($ 247 billion), Amazon (1 trillion), Cisco ($ 204 billion), Nvidia ($ 163 billion) and many more.[41]

2.3 IoT market pandemic effects

The 'Internet of Things' market is characterized by a segmentation/subdivision of customer needs into heterogeneous groups, each of which is satisfied by a specific good or service. Some of the main factors on which the segmentation of the IoT market is based are hardware, software and cloud services, each of which has been affected differently by the COVID-19 pandemic: For example in 2020, despite the difficulties, the global spending in the hardware and IoT services grew by 5.4% and 34.7%, respectively. However, due to the coronavirus pandemic, corporate investments in the IoT sector have

[39] "Internet of Things (IoT) Market, By Software (Data Management, Network Management), By Hardware(Sensors, camera), By Services (Manage Services, Professional Services), By Organization Type (Small and Medium Scale Business, Large Scale Business) - Forecast 2027", in Market Research Future, available at https://www.marketresearchfuture.com/reports/internet-of-things-market-1176#answer6 (last visited 4/09/2021).

[40] "Global Internet of Things (IoT) Market 2021 Is Expected To Register a CAGR Of Growing rate% With Top Countries Data to Showing Impressive Growth by Industry Trends, Share, Size, Top Key Players Analysis and Forecast Research", in WBOC Delmarva's News Leader, available at https://www.wboc.com/story/44138245/global-internet-of-things-iot-market-2021-is-expected-to-register-a-cagr-of-growing-rate-with-top-countries-data-to-showing-impressive-growth-by (last visited 4/09/2021).

[41] "Top 30 maggiori aziende tech statunitensi 2020" [Top 30 largest US tech companies], in DISFOLD, available at https://it.disfold.com/top-aziende-tech-statunitensi/#nvidia (last visited 4/09/2021).

slowed significantly due to cooling supply chains and travel difficulties that have held back IoT component installations in cities and smart business facilities. As for the software market segment, it suffered a negative impact even of less magnitude than that recorded by the other two, especially as regards the useful tools within the pandemic context. Within the same background, the nation that was most successful in containing the impact of the 'corona' pandemic was China: corporate national spending in the IoT industry grew by 23.5% (about double the average).[42]

Although the health emergency has had a decidedly negative effect on the global economy, causing periods characterized by serious economic problems for companies active in any sector, the IoT industry has had a clearly less negative impact than the others. In fact, it can be said that the coronavirus has definitively consecrated the IoT, once again underlining the importance of this technology both in the corporate and individual spheres: during the pandemic period the IoT played a crucial role in tracing the virus in the population, with the use of advanced IoT solutions such as that of connected thermal cameras aimed at detecting potentially infected people within the same structure.[43] Other examples of IoT solutions applied to the pandemic context are: (i) the tracking of population movements through the cell phone localization function, in order to be able to trace the contagion chain more easily; (ii) the support for food shopping for people infected with COVID-19 through services offered by companies such as *Glovo* or *Frescofrigo*, in order to avoid the spread of the virus; (iii) the delivery of the goods through robotic vehicles with autonomous driving i.e., without a driver (e.g., *Neolix)*.[44]

2.4 IoT privacy and risks

The causes of the general decline in the growth rate found on the Internet of Things market since 2020 concern, in addition to the COVID-19 pandemic, the risks and shortcomings regarding the protection of sensitive data and privacy. In fact, the simplicity of the IoT structure and the electronic components of its smart devices continually

[42] P. Wegner, *op.cit.*

[43] GlobalData, *op.cit.*

[44] G. Salvadori e A.Tumino, "L'Internet of Things ai tempi di Covid-19: servizi di valore per cittadini e imprese" [The Internet of Things in the time of Covid-19: valuable services for citizens and businesses], in Politecnico Milano, available at https://www.som.polimi.it/linternet-of-things-ai-tempi-di-covid-19-servizi-di-valore-per-cittadini-e-imprese/ (last visited 4/09/2021).

exposes them to the danger of cyber-attacks conducted by hackers who, by illegally penetrating a computer network, abusively use the data and information contained therein. Furthermore, in a context of great expansion and development, with billions of devices connected to an Internet network, cybercriminals can more easily and regularly access the vast pool of poorly protected data produced within the network, exploiting its vulnerability to manipulate and make them usable only in exchange for a cash ransom.[45]

The first major case of an IoT attack dates back to 2016, when a malware (Mirai) released a source code that allowed anyone to create their own Botnet formed by IoT devices i.e., a computer network managed by a master-bot composed of vulnerable devices (not configured by default) infected with specialized malware.[46] The cyber-attack occurred when a botnet, made up of some of these devices, attacked the database of Dyn, a company that offered services to protect and optimize online infrastructures.[47]

Mirai's was not the only case of a cyber-attack. In fact, according to a study conducted by the research and analysis company in the field of information technology Gartner, about one company in five has suffered in the last three years at least one cyber-attack linked to the IoT devices present in its facilities. The issue of cybersecurity, therefore, does not only concern the mobile devices and computers used by the firm employees, but also all those objects connected to the internet within the structure that deal with collecting sensitive data and that play a fundamental role in the management of the business development and production.[48]

The main causes behind cyber-attacks that constantly endanger the security of consumers of IoT devices can be classified as: (i) lack of compliance by IoT manufacturers who do not spend sufficient resources on the security of integrated IT

[45] A.S. Gillis (2020), "Internet of Things (IoT)", in IoT Agenda, available at https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (last visited 4/09/2021); P. Todorovich, *op.cit.*

[46] "Botnet", in Wikipedia, The Free Encyclopedia, available at https://it.wikipedia.org/wiki/Botnet (last visited 4/09/2021).

[47] "Dyn (company)", in Wikipedia, The Free Encyclopedia, available at https://en.wikipedia.org/wiki/Dyn_(company) (last visited 4/09/2021); A. Grau, "Mirai Botnet Shows Just How Vulnerable the IoT Really Is", in Icon Labs, available at http://www.iconlabs.com/prod/mirai-botnet-shows-just-how-vulnerable-iot-really-0 (last visited 4/09/2021); P. Todorovich, *op.cit.*

[48] M. Bellini, *op.cit.*

components; (ii) lack of awareness of the danger on the part of the user; (iii) Security flaws in system updates of IoT devices.[49]

In order to counter the increasingly pressing problem of security in this sector, it is necessary to take into account that any connected device is exposed to a potential cyber risk. Each device, in fact, before being placed on the market and connected to the network, must be protected by effective and systematically updated security systems in order to guarantee the necessary protection for its consumers.[50] The defence methods that concern the consumer, on the other hand, consist in paying particular attention to the configuration processes of the devices, to the periodic updating of the operating systems and to the choice of reliable and authorized IoT products. Other general indications concern the strengthening of the encryption tools for sensitive data and also of the internet in the phases of authentication, control, authorization for new accesses, and data retention. In addition, particular attention must be paid to the in-depth study of the prevention of potential hacker attacks. The IoT devices that manage corporate environments, in fact, regularly collect and send sensitive data about the security of systems and accesses, making it essential, first of all for manufacturers and then for companies, a greater investment in the prevention of cyber threats and in the research of increasingly sophisticated protection methods.[51]

However, the laws governing the privacy and security of the IoT industry are still unclear. In fact, since there is no law that specifically refers to IoT devices, we must rely on general privacy laws, sometimes obsolete and difficult to apply to a new and constantly evolving sector.[52]

[49] "Top 10 biggest IoT Security Issues", in intellectsoft, available at https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (last visited 4/09/2021).

[50] M. Bellini, *op.cit.*

[51] *Ibid*.; P. Todorovich, *op.cit.*

[52] A. Talbott, "Privacy Laws: How the US, EU and others protect IoT data (or don't)", in ZDNet, available at https://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/ (last visited 4/09/2021).

CHAPTER 3: MAIN IOT SECTOR COMPETITION FEATURES

3.1 The IoT sector in the crosshairs of the EU Antitrust

The strong expansion that the IoT industry is experiencing in recent years has prompted the European Commission to focus for the first time on the mechanisms and laws that regulate competition within this sector. In fact, on 16th July 2020, the Commission itself launched an antitrust investigation on the ‘Internet of Things’ sector with regard to products serving consumers within the European continent.[53] The survey follows the new digital plan of the European Union which takes the name of *Shaping Europe's Digital Future*, according to which, with the passage of time, there is an increasing need for companies and the public administration to mature the awareness that the digital is a powerful and essential tool for the delineation of effective business strategies. The goal is to raise awareness and to encourage a renewal in the digital field in the next five years in step with that of the giants United States and China, through the provision of useful equipment in order to convert the processes of production and processing of data from traditional forms to digital ones.[54]

The investigation launched by the European Commission will flow into future interventions of the IoT market. In particular, it concerns the consumer market of products and services equipped with technologies that allow it to connect to an internet network. In fact, the sector inquiry is closely interested in IoT products such as those discussed in the previous chapters: wearable devices, voice assistants and connected

[53] P. Johnson, K. Haegeman, S.J. Mobley and N. Kredel, “European Union: European Commission Launches a Sector Inquiry into the Consumer Internet of Things”, in GLOBAL COMPLIANCE NEWS, available at https://www.globalcompliancenews.com/2020/07/30/european-commission-launches-a-sector-inquiry-into-the-consumer-internet-of-things-27072020/ (last visited 4/09/2021); “IoT: la Commissione UE avvia un’indagine antitrust” [IoT: the EU Commission launches an antitrust investigation], in Confindustria Radio Televisioni, available at https://confindustriaradiotv.it/iot-la-commissione-ue-avvia-unindagine-antitrust/ (last visited 4/09/2021).

[54] P. Del Castillo, “Shaping Europe’s digital future”, in The European Files, available at https://www.europeanfiles.eu/digital/shaping-europes-digital-future (last visited 4/09/2021); “Il nuovo Piano digitale dell'Unione Europea: cosa prevede” [The new digital plan of the European Union: what it foresees], in Italiaonline, available at https://www.italiaonline.it/risorse/il-nuovo-piano-digitale-dell-unione-europea-cosa-prevede-1029 (last visited 4/09/2021).

devices used in the business and home context (e.g., lighting systems, wireless home automation, heating systems). The research also aims to collect information on the multiple services accessible exclusively through the use of the IoT devices themselves (e.g., video streaming services), involving both producers and consumers.[55]

As mentioned above, the reasons that have led the European Commission to take a greater interest in the events concerning the competition within the IoT market are ascribed to the exponential growth that the IoT sector has had in recent years, and that presumably will continue to record in the next five years (e.g., the number of voice assistants is destined to double from 4.2 billion in 2020 to 8.4 billion in 2024). In this regard, the executive vice-president of the European Commission, who is responsible for his duties in the field of competition policy, expressed himself on the matter, declaring that:

> *The consumer Internet of Things is expected to grow significantly in the coming years and become commonplace in the daily lives of European consumers. […] The possibilities seem endless, and the access to large amounts of user data appears to be the key for success in this sector. For this reason we have to make sure that market players are not using their control over such data to distort competition. In this sense, this sector inquiry will help us better understand the nature and likely effects of the possible competition problems in this sector.*[56]

These statements do not deny and certainly do not place limits on the potential that technological advancement has for a progress that goes beyond mere economic gain for industries and governments. On the contrary, they reinforce even more the importance that IoT technology has in our lives, aiming to guarantee its development in the name of quality, and (above all) that responds to the needs of its customers. Therefore, moving in such a way that markets remain open and competitive avoids the possibility of entering a loop of mediocrity within which the quality of the devices and the needs of customers do not guide decisions. In fact, the thing to avoid is that companies with greater economic

[55] "Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT)", in European Commission, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326 (last visited 4/09/2021).

[56] *Ibid*.

availability distort the market by overcoming the equilibrium point beyond which competition turns into a monopoly.[57]

The aim of the action is to acquire a more in-depth and aware knowledge about competition on the 'Internet of Things' sector, and consequently understand if the competitive mechanisms of this market go in the same direction of the antitrust rules of the European Union. In this way, the European Commission will aim to have a clearer picture of the practices adopted by the many companies operating in the IoT industry, with the aim of countering illegal practices such as those aimed at limiting the access of third-party companies to data collected by IoT devices.[58]

The survey will be based on data collected on about 400 operating companies and smart devices producers in the IoT sector from the continents of Europe, Asia and America. In the event that the inquiry results identify competitive problems within the IoT market, it will be up to the Commission to ensure that EU antitrust rules are complied with by all companies involved under Articles 101 and 101 of the Treaty on the Functioning of the European Union (TFEU), which prohibit anti-competitive agreements and concerted practices between companies, as well as abuses of dominant positions.[59]

3.2 Consumer IoT sector competition parameters

According to the data collected by the European Commission from the companies interviewed, the parameters and characteristics of IoT devices to be considered when manufacturing companies compete with others for the integration on/interoperability with

[57] "The internet of things: a new path to European prosperity", in KEARNEY, available at https://www.kearney.com/digital/article?/a/the-internet-of-things-a-new-path-to-european-prosperity (last visited 4/09/2021); McKinsey&Company, "The Internet of Things: How to capture the value of IoT", in mckinsey.com, available at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20How%20to%20capture%20the%20value%20of%20IoT/How-to-capture-the-value-of-IoT.pdf (last visited 4/09/2021); Redazione ImpresaCity, "Antitrust: il mercato IoT nel mirino della Commissione Europea" [Antitrust: the IoT market in the sights of the European Commission], in impresacity, available at https://www.impresacity.it/news/23907/antitrust-mercato-iot-commissione-europea.html (last visited 4/09/2021).

[58] *Ibid*.

[59] "Antitrust", in European Commission, available at https://ec.europa.eu/competition-policy/antitrust_en (last visited 4/09/2021).

other smart home devices, consumer IoT services and voice assistants vary depending on the manufacturing branch in which the company operates within the 'Internet of Things' industry.[60]

In particular, producers of smart home devices argue that the main parameters that confer a competitive advantage to IoT devices developed by companies operating in their market segment for the contention of the integration on other smart home devices, consumer IoT services and voice assistants, in order of incisiveness, are: (i) the quality, (ii) the cyber-security, (iii) the brand reputation, (iv) the privacy policy, (v) the technical support services, (vi) the languages availability, and (vii) advertising possibilities.[61]

As for the manufacturers of voice assistants, they similarly argue that the main parameters of voice assistants to compete with other voice assistants for the integration on third-party smart devices are: (i) the quality, (ii) the reputation of the brand, (iii) the privacy policy, (v) the cybersecurity, (vi) technical support services, (vi) the languages availability, and (vii) advertising possibilities.[62]

Instead, from the data collected by consumer IoT service providers it can be said that the main factors to compete with other consumer IoT services for the integration on third-party smart devices are: (i) the quality of the service, (ii) the brand reputation, (iii) the number of users of the consumer IoT service, (iv) the cybersecurity, (v) the privacy policy, (vi) the availability of languages, and (vii) advertising possibilities.[63]

Rather, to acquire a competitive advantage from the point of view of direct competition for consumers, in each market segment other parameters emerge and acquire greater relevance, such as: (i) the user-friendliness, (ii) the price, (iii the energy consumption, (iv) the phone connectivity, (v) the range of payment options.[64]

3.3 Barriers to entry/expansion

The investigation carried out by the European Commission also revealed the elements that represent an obstacle to competition on the ‘Internet of Things’ market. These are the so-called barriers of entry and expansion that complicate the entry into the

[60] European Commission, *op.cit.*, p.39
[61] *Id.*, p.40
[62] *Id.*, p.41
[63] *Id.*, p.43
[64] *Id.*, p.44

IoT market of new existing companies and/or the expansion for active companies already operating in the market.[65]

From the data collected it emerges that in each production subsector of the IoT market (smart home devices, wearable devices, voice assistants and IoT consumer services), the entry and expansion barriers that represent a major impediment factor for new/already operating companies in the IoT industry, in order of importance, are: the cost of the technology investment, the competitive pressure, the lack of interoperability with relevant third-party smart devices, the lack of interoperability with other relevant third-party technology, the lack of interoperability with home automation systems, the lack of interoperability with relevant third-party voice assistants, and regulatory barriers.[66]

Analyzing the costs of technological investments as the greatest barrier of entry for companies that try to set up their business on an activity in force within the IoT sector, it can easily be guessed how those for the development of data processing and cloud storage infrastructures are often impossible to sustain for companies with limited economic availability. In particular, the entry barrier represented by the costs for technological investments acquires even more strength and solidity in correspondence with the development and consumption of generic voice assistants (e.g., Alexa). The integration of voice assistants with incompatible operating systems of third-party providers is also very expensive.[67]

The high costs that companies have to bear to become part of the 'Internet of Things' market often lead small companies to rely on the digital infrastructures of giants such as Amazon and Google to break down the barrier of entry for investments in technology by gaining access to cloud services developed by third parties. However, while this breaks down the investment cost barrier, the interoperability of data processed in different clouds raises an additional barrier that complicates new existing companies from entering/expanding within the IoT industry.[68]

[65] A. Hayes, "Barriers to Entry", in Investopedia, available at https://www.investopedia.com/terms/b/barrierstoentry.asp (last visited 4/09/2021).

[66] European Commission, *op.cit.*, p.47

[67] *Id.*, p.48

[68] *Ibid.*

3.4 The Big Techs' shadow

Although the IoT sector has emerged decisively only in recent years, in conjunction with the growth and advancement of new cutting-edge technologies, it is still characterized by important network externality effects that give a significant competitive advantage to established digital ecosystems by speeding up their rooting process within the market.[69] In this regard, also on this occasion, the executive vice-president of the European Commission, Margrethe Vestager, said that "*when they launched this sector inquiry, they were concerned that there might be a risk of gatekeepers emerging in this sector, and that they were worried that they could use their power to harm competition, to the detriment of developing businesses and consumers*".[70]

The main competitors that could exploit their dominance to harm competition at the expense of companies active in each of the four consumer IoT segments are basically Amazon, Google and Apple. In fact, these brands have obtained a positioning within the 'Internet of Things' market of a certain importance, and consequently are able to address consumer preferences regarding the consumption of certain products and services. In light of this, the biggest stumbling block preventing the growth and expansion of companies providing IoT products and services is represented by multinationals (Amazon, Google and Apple) that offer the same type of product or service with which small businesses are not able to compete.[71]

However, analyzing the importance that these big tech giants have for innovation and for the introduction of new modes of designation and production within the IoT sector, Luca Schiavoni, telecommunications and technology analyst at the analysis company *Assembly Research*, said that:

> *Regulating those three companies may not necessarily result in a better consumer IoT market. Moreover, we can't be sure that forcing Big Tech platforms to be more 'neutral' will necessarily lead to better outcomes. The jury is still out there on whether enforcing interoperability in this market would really be a good thing for*

[69] L. Clarke, "The EU could intervene to curb Big Tech's IoT market dominance", in TECH MONITOR, available at https://techmonitor.ai/policy/big-tech/big-tech-and-iot-eu-apple-google-amazon (last visited 4/09/2021).

[70] E. Johansson, "Tech giants are harming IoT competition, says EU", in VERDICT, available at https://www.verdict.co.uk/tech-giants-are-harming-iot-competition-says-eu/ (last visited 4/09/2021).

[71] European Commission, *op.cit.*, p.48-49

> *consumers. In fact, it could increase complexity, which could impact products' usability, and even raise privacy risks.*[72]

3.5 A brief expansion strategies' overview

Despite the difficulties posed by the presence of the Big Tech colossi which distort competition, and by the presence of the barriers to entry and expansion that characterize the IoT market that we discussed in the previous paragraph, there are various expansion strategies that most companies use to ease the growth of their business. In fact, from the data collected by the European Commission, it is clear that in the last four years a good number of companies (16.5%), objects of the sector inquiry, have acquired control of the production plants of another company and/or have stipulated a joint venture contract to expand their range of action with the aim of exploiting a greater effect of economy of scale.[73]

However, there are also other strategies that aim to facilitate the entrance into the IoT market and/or to increase the level of the business of a company in terms of turnover, quantity of audience involved, and quality of products and services offered to customers. The most common strategy is to enter into commercial agreements with other companies active in the sector, with the aim of reaching a wider audience to which to propose and promote IoT products and services through a greater integration on/interoperability with other operating systems. These agreements include revenue sharing, co-branding, bundling, and exclusivity.[74]

Some examples of what is described above are the vast number of IoT product and service providers who have created business relationships with suppliers belonging to the same sector through revenue-sharing strategies that include commissions based on the amount of customers coming from their traffic channels.[75]

[72] L. Clarke, *op.cit.*

[73] European Commission, *op.cit.*, p.49

[74] *Id.*, p.49-50

[75] *Id.*, p.50

CHAPTER 4: AREAS OF POTENTIAL CONCERNS

4.1 Pre-installation and visibility concerns

In the previous chapter we explored the main parameters and elements that feed the general competitive mechanisms within the IoT industry. However, by delving even further into the issues that negatively impact competition in the IoT consumer sector, the industry survey revealed further structural complexities that can potentially hinder innovation and distort consumer choices. We will discuss them in this section.

The problem we are going to talk about in this paragraph concerns consumer IoT services with a particular focus on distortive practices that deal with their pre-installation on smart devices. In fact, it is in the eye of the storm every practice that confers a competitive advantage aimed at increasing the visibility, the popularity and the perceived value of an IoT service provided by companies favorably positioned within the market, at the expense of smaller local companies or with less notoriety. In fact, all those actions that involve an embryonic phase of pre-setting the relevant consumer IoT services within smart devices and/or voice assistants, which have the objective of directing the user towards a more rooted use of the company's products and services, are considered to be of common fulfillment. This practice mainly involves internationally renowned companies such as Amazon, Google and Apple which, taking advantage of their infrastructure and a solid production chain, offer their services by default on the smart devices/voice assistants they manufacture (e.g., Amazon offers predefined consumer IoT services integrated within their Alexa voice assistant).[76]

However, especially in the event that a company does not own a proprietary IoT services' provision, that company, producer of smart devices, may also consider supplementing its products with services provided by third-party companies. This usually happens in short periods of time in conjunction with particular contexts (e.g., advertising propaganda). The evaluation criteria on which the choice of one IoT service provider over another is based may vary, and also the selection processes are not always transparent. However, the parameters that are usually considered are: the quality of the service offered, the users' past preferences, and the exclusivity of the service.[77]

[76] European Commission, *op.cit.*, p.111-116

[77] *Ibid.*

In this context, the default deployment mechanisms vary according to the prominence arrangements agreed between smart device manufacturers and consumer IoT service providers. Therefore, a differentiation must be made between preloaded features and pre-downloaded features: while the former involve a total installation on the device and do not require further actions by the user, the latter need a download to be unlocked. In fact, IoT service providers often haggle with smart device manufacturers on the positioning, features, and the ways in which their service should be integrated and presented on the third-party device. Often, this concerns the inclusion of the logo of the company providing the service, with the aim of increasing the availability and popularity of the brand. Or instead, it may involve hardware features (not reconfigurable by users) such as giving greater prominence to buttons that provide instant access to specific consumer IoT services.[78]

The main problem that emerged from the sector inquiry, which involved about 400 companies operating within the IoT industry, lies in the fact that a good chunk of respondents admitted that most consumer IoT service providers do not have the economic possibilities to make arrangements that include the default installation of their services on smart devices produced by other companies. In fact, these agreements provide for onerous cash payments, or the agreement on percentages of revenue distribution that prevent smaller companies from recouping investment costs. Therefore, despite the opportunity of obtaining a relevant positioning for consumer IoT services on smart devices produced by third parties, with the aim of reaching a wider and interested audience, pre-installation practices mostly represent a competitive disadvantage for minor providers of such services. This is because they do not have the economic and structural resources to show their services to a wider audience through IoT devices of other manufacturing companies, with a consequent increasing of the already wide differences between large companies and local ones. In fact, a user, to be able to access services not pre-installed, will have to renounce to use the services included in the package of the purchased smart device and, subsequently, take further steps to access a service not included in the offer. As a result, the user will prefer to use services with a higher level of availability, at the expense of those that have less accessibility and that require a greater effort of use. This goes obviously to the advantage of large companies, and to the

[78] *Ibid.*

disadvantage of smaller companies that cannot afford to pre-install their applications on a third-party smart device and/or a voice assistant.[79]

In addition, the competitive disadvantage also concerns the access to data. In fact, companies that do not have the opportunity to pre-install their applications on a third-party smart device and/or a voice assistant will also have less data available on the target audience than giants such as Amazon, Google and Apple, and will therefore not be able to offer a service as qualitative, desirable and equally responsive to the customer needs.[80]

4.2 Lack of platforms interoperability

Another topic much discussed in the competition field is that related to the interoperability of IoT platforms. In particular, there are two main problems encountered: (1) problems related to the integration of IoT products with the available compatible technological platforms; (2) concerns related to the wide difference between the level of performance recorded by the integrated services provided by third parties on these technological platforms, and the level of performance of the services provided by the IoT platform providers themselves.[81]

Before delving into the details of the problems encountered by the antitrust investigation on competition about the interoperability of technological platforms, let's briefly explain what is meant by *consumer IoTplatform*: it can be traced back to any voice assistant or operating system that collects different hardware and software elements (e.g., sensors, gateways, internet networks, data analysis and processing software) in a single ecosystem, in order to allow these elements to interact with each other and increase their complementarity. In this context, tech giants such as Google, Amazon and Apple are called *gatekeepers*. This nickname is mainly due to the fact that they are the providers of the main IoT technology platforms. This privilege allows them to control and determine which operating systems and voice assistants really deserve the access to them. The selection process takes place through an evaluation of certain contractual (and technical) requirements imposed by the suppliers of the IoT platform itself. For example, at the technical level, manufacturers of IoT devices are bound to adapt their products based on software and hardware specifications established by the operating system vendor. At the

[79] *Ibid.*
[80] *Ibid.*
[81] European Commission, *op.cit.*, p.102-106

contractual level, IoT device manufacturers are expected to adhere to terms and conditions imposed by the platform providers.[82]

In light of what has been said so far, the first problem encountered by the respondents surveyed derives from the fact that the platforms are not all the same, and that the lack of standard and homogeneous technical solutions for the fulfillment of the integration requirements imposed makes the simultaneous adaptation of the characteristics of IoT devices to each platform very difficult and expensive in terms of time and money. The main cause of this difficulty is represented by the difference in the APIs (Application Programming Interfaces) that each technological platform makes available. In fact, since the API is a unique programming interface for each IoT platform provided by its developers to allow programmers of other applications to have access and use it successfully (e.g., Google releases the API in order to allow other programmers to integrate their applications with Google services)[83], many of the device manufacturers and IoT service providers believe that the strong heterogeneity of compatibility processes leads only to a significant increase in the integration costs and to an increase in the overall complexity of interoperability. This is because manufacturers of technological devices do not have the possibility to develop software (or applications) that are able to exploit multiple platforms at the same time. As a result, the entry into the IoT market of new products and/or services is also severely slowed down. In addition, the technological fragmentation of IoT platforms, and all the issues related to it, hinder IoT solutions' manufacturers in offering a user experience of equal quality on multiple platforms simultaneously.[84]

The second problem, as mentioned above, concerns the gap in terms of performance between the integrated services provided by third parties on technological platforms, and the services provided by the IoT platform providers themselves. This

[82] *Ibid*.

[83] *Ibid*.; "What is an API? (Application Programming Interface)", in MuleSoft, available at https://www.mulesoft.com/resources/api/what-is-an-api (last visited 4/09/2021); C. Hoffman, "What Is an API, and How Do Developers Use Them?", in How-TO Geek, available at https://www.howtogeek.com/343877/what-is-an-api/ (last visited 4/09/2021); "API: cosa c'è da sapere sulle interfacce di programmazione" [API: what you need to know about programming interfaces], in Digital Guide IONOS, available at https://www.ionos.it/digitalguide/siti-web/programmazione-del-sito-web/che-cose-unapi/ (last visited 4/09/2021).

[84] European Commission, *op.cit.*, p.102-106

situation significantly distorts competitive mechanisms, as the high level of performance efficiency of company's IoT products and services is considered an indispensable requisite to compete successfully within the consumer IoT sector. For this reason, the main providers of IoT technology platforms are incentivized to restrict some third-party products and services' functionalities, hindering their attempt to offer services of their own quality. In addition, the dominant position of the tech giants, aiming to condition, penalize and reduce the already limited margins that smaller companies have to make room in the IoT industry market, threatens to definitively extinguish any development and innovation attempt by many IoT device manufacturers and service providers.[85]

4.3 Data accessibility concerns

A further issue that generates particular apprehension in the minds of the respondents concerns the considerable advantages that voice assistant providers have in the collection of data from the consumers' use of third-party IoT products and services. In fact, providers of voice assistants have a preferential track regarding accessibility to data not accessible by other providers, allowing them to develop differentiated and more efficient communication strategies that can break down competition. In particular, they are the only providers that are given access to the immense amount of data generated from the voice queries daily applied in the search engines by consumers belonging to all the segments of the IoT industry market. Specifically, this allows them to have more information available to analyze than the competition, and consequently to take competitive and effective actions aimed at annihilating any effort dedicated to the obtaining of a competitive advantage by companies operating in the IoT consumer sector. This concept was explained with the following words by one of the CEOs of the companies surveyed:

> Access to relevant data is key to sustain the design and development of new [...] devices or solutions. Being able to access to customer behavior data and operational data from the market itself and related markets from different products and brands constitutes a huge competitive advantage. The advantage in this regard offered to companies in a gateway function [...] such as Voice Assistants is enormous. It is clear that these companies have a paramount competitive advantage over, not only new entrants, but over the rest of the players in the sector that will not be able to access to such sources of information in a similar way.[86]

[85] *Ibid.*

[86] European Commission, *op.cit.*, p.110-111

The competitive disadvantage of smart device manufacturers and third-party service providers is strengthened by the fact that they have the permission, by the main providers of voice assistants, to access to a very limited pool of data from sources that are, moreover, not attributable (anonymous). The limited access to an amount of low-quality data increases the concerns and the gap on the competitive and development front between the voice assistant providers and the other ones.[87]

Particular concerns have been recorded by the main players active in the consumer IoT sector also in terms of privacy and security. In particular, smart home device manufacturers have criticized the unlawful impositions, to which they are subjected, to distribute data about the condition of their smart devices to voice assistants' providers. This constraint, in addition to further distorting competition, goes decisively against the development and growth of this sector, as it strongly discourages companies to integrate their own IoT services with the voice assistants of the main suppliers of the industry, causing a significant reduction in the overall quality of services offered to consumers.[88]

Another situation being evaluated by the European Commission in antitrust matters, also this one related to the data obtained from the consumers' use of IoT products and services, concerns the monetization of information through simple online advertising campaigns carried out by the main IoT technology platforms' providers. This framework is problematic as it generates a further increase of the entry barriers for smaller companies that are not able to compete with such important realities. In fact, data monetization itself allows big companies to have a greater amount of funds available to be used to finance investments aimed at improving their offer, so allowing them to expand furthermore their presence within all the segments of the IoT industry.[89]

4.4 Leading providers disintermediation concerns

Concerns have also been raised on the dependence that most entrepreneurs who have started a manufacturing business in the IoT industry have towards the major voice assistants and smart device operating systems' providers. In fact, since the latter act as intermediaries between the user and the "minor" suppliers through the user interfaces they make available, the respondents expressed many perplexities, and a deep apprehension,

[87] *Ibid.*
[88] *Ibid.*
[89] *Ibid.*

about the concrete possibility of losing (1) the recognizability of their brand and (2) any type of personal relationship with their users, including any type of control over the practices of ascertaining the qualitative level of the experience lived by the client.

The underlying mechanism of this is triggered by the imposition by the major IoT technology platform providers of their user configuration and monitoring processes on third parties, when new smart devices are first connected to the net. Even worse, most of the time, users are required to create their own personal account within the digital operating system, or an identification ID code, as a prerequisite for gaining access to the functionalities of third-party smart devices and consumer IoT services.

Consequently, this prevents third-party providers from having a direct communication thread with their consumers, and also denies them the moral right to collect relevant data, generated by the user experiences, about the products/services they have manufactured/offered. All this is then inevitably negatively reflected in the after-sales communication strategies aimed at the client loyalty. In contrast, major providers of consumer IoT technology platforms have the enormous competitive advantage of having no constraints or restrictions in monitoring the user experience in relation to the use of their products and/or services. In fact, the interaction with the user takes place continuously, allowing companies to collect all the relevant information useful for the development of effective pre- and post-sales marketing and communication strategies.[90]

[90] European Commission, *op.cit.*, p.117, p.122

CONCLUSION

As already explained above, this thesis aimed to highlight and examine in detail all those problems and gaps that the ‘Internet of Things’ industry presents with regard to the protection of competition and the possible abuses of dominant positions of important companies such as Amazon, Google and Apple. In particular, the thesis has developed by making extensive reference to the sector inquiry carried out by the European Commission in antitrust matters, of which, to date, only a preliminary report has been published with the aim of encouraging interested parties to exchange their points of view. In this regard, by 1 September 2021, the companies interviewed had to gather their opinions on the matter, so that the European Commission can publish a final version of the report within the first half of 2022.[91]

The feeling is that the Directorate-General for Competition (DG COMP) will have to take advantage of all the information that emerged during the investigation and introduce as soon as possible functional and effective regulations aimed at protecting minor business realities. Otherwise, the obstacles that do not allow companies to compete at high performance within the IoT market, as well as harming consumers in terms of choice, risk stifling innovation in the sector.

[91] European Commission, *op.cit.*, p.123

BIBLIOGRAPHY AND SITOGRAPHY

1. https://www.internet4things.it/iot-library/internet-of-things-gli-ambiti-applicativi-in-italia/
2. https://iot-analytics.com/internet-of-things-definition/
3. https://www.zerounoweb.it/analytics/big-data/internet-of-things-iot-come-funziona/
4. https://www.techaheadcorp.com/knowledge-center/evolution-of-iot/
5. https://www.rfidjournal.com/that-internet-of-things-thing
6. https://www.greenvulcano.com/iot-what-to-expect-in-the-future/
7. https://itmanager.space/internet-of-things/
8. https://www.ericsson.com/en/future-technologies/future-iot
9. https://www.simoniot.com/history-of-iot/
10. https://www.ingenio-web.it/23301-introduzione-al-mondo-dellinternet-of-things
11. https://www.digi.com/blog/post/the-4-stages-of-iot-architecture
12. https://it.wikipedia.org/wiki/Network
13. https://en.wikipedia.org/w/index.php?title=User_interface&oldid=1031291510
14. https://ec.europa.eu/competition-policy/system/files/2021 06/internet_of_things_preliminary_report.pdf
15. https://www.i-scoop.eu/internet-of-things-guide/what-is-consumer-internet-of-things-ciot/.
16. https://www.behavioraleconomics.com/three-ways-the-internet-of-things-is-shaping-consumer-behavior/
17. https://blog.osservatori.net/it_it/modellazione-predittiva-come-funziona
18. https://www.agingproject.uniupo.it/glossario/studio-randomizzato-controllato/
19. https://www.ontotext.com/knowledgehub/fundamentals/dikw-pyramid/
20. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/
21. https://www.eetasia.com/global-iot-market-to-surpass-1-trillion-mark-by-2024/
22. https://www.marketresearchfuture.com/reports/internet-of-things-market-1176#answer6
23. https://www.wboc.com/story/44138245/global-internet-of-things-iot-market-2021-is-expected-to-register-a-cagr-of-growing-rate-with-top-countries-data-to-showing-impressive-growth-by
24. https://it.disfold.com/top-aziende-tech-statunitensi/#nvidia
25. https://www.eetasia.com/global-iot-market-to-surpass-1-trillion-mark-by-2024/
26. https://www.som.polimi.it/linternet-of-things-ai-tempi-di-covid-19-servizi-di-valore-per-cittadini-e-imprese/

27. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

28. https://it.wikipedia.org/wiki/Botnet

29. https://en.wikipedia.org/wiki/Dyn_(company)

30. http://www.iconlabs.com/prod/mirai-botnet-shows-just-how-vulnerable-iot-really-0

31. https://www.intellectsoft.net/blog/biggest-iot-security-issues/

32. https://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/

33. https://www.globalcompliancenews.com/2020/07/30/european-commission-launches-a-sector-inquiry-into-the-consumer-internet-of-things-27072020/

34. https://confindustriaradiotv.it/iot-la-commissione-ue-avvia-unindagine-antitrust/

35. https://www.europeanfiles.eu/digital/shaping-europes-digital-future

36. https://www.italiaonline.it/risorse/il-nuovo-piano-digitale-dell-unione-europea-cosa-prevede-1029

37. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326

38. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326

39. https://www.kearney.com/digital/article?/a/the-internet-of-things-a-new-path-to-european-prosperity

40. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20How%20to%20capture%20the%20value%20of%20IoT/How-to-capture-the-value-of-IoT.pdf

41. https://www.impresacity.it/news/23907/antitrust-mercato-iot-commissione-europea.html

42. https://ec.europa.eu/competition-policy/antitrust_en

43. https://www.investopedia.com/terms/b/barrierstoentry.asp

44. https://techmonitor.ai/policy/big-tech/big-tech-and-iot-eu-apple-google-amazon

45. https://www.verdict.co.uk/tech-giants-are-harming-iot-competition-says-eu/

46. https://www.mulesoft.com/resources/api/what-is-an-api

47. https://www.howtogeek.com/343877/what-is-an-api/

48. https://www.ionos.it/digitalguide/siti-web/programmazione-del-sito-web/che-cose-unapi/