LUISS

Department of Business and Management
Bachelor's Degree in Management and Computer Science
Chair of Business Law and ICT

"The impact that Data Collection has on social control on Democratic Nations: Political Microtargeting & the Facebook/Meta Case"

Prof. Andrea Giannaccari
RELATORE

Matr. Carlotta Conversi 239421
CANDIDATO

Anno Accademico 2021/2022

Table of Contents

Abstract

Nowadays the world that we know is in continue evolution: nothing that we know today will count in few years. It could seem like a paradox or, better, an artifact but it is nothing less than the truth.

Everything is subject to change and the speed at which it takes place is incredible.

Although we could be astonished about the development of our society, it is important to highlight the methodologies under which our world is regulated.

Of course, this topic could be considered in a worldwide prospective, but in this paper, we are going to take into consideration only countries where democratic governments have been established: USA and UE (with a deeper view on Germany and Italy).

To introduce the topic about which this thesis is about I want to point out a person, which maybe could also be seen under the light of, for some people, a modern “superhero”: Edward Snowden.

The story of this man could summarize the ethical problems that we are facing nowadays when we talk about microtargeting.

As we will see, microtargeting is a technique through which profiling takes place.

It is largely used and it allows to identify the users’ interests in order to influence their actions and control their behaviors.

Whether you are a criminal or a normal person, whether you have done something dangerous in your life or not, you will be subject to microtargeting.

This is an action that occurs every day to every person (physical or legal) that interacts with the network.

Is it fair?

Thanks to Edward Snowden the entire world has had the opportunity to discover that USA, through the help of NSA and CIA were targeting almost every person in America.

There was a time while they discovered that the percentage of people that was targeted in America was almost three times the one that was taken into consideration in Russia.

Projects that were born in order to balance the complex political axis between nations, were used to control people in their own country.

The report of Edward Snowden does not only revalue the whole American’s system but showed us also the powerfulness of these kind of means that, under wrong hands, can really have a catastrophic impact.

In my analysis I won't focus on an American former computer intelligence consultant, but on a platform that has had many complains and was known under the name of Facebook and now is called Meta.

This name has behind it many people from both size: analyzer and analyzed. Meta is not only a platform, neither only a name, but it is a reality.

Since the topic of social control performed in nowadays society is too extensive and could imply to many factors, this thesis will go into detail on how social control has been implemented by the innovative phenomenon that Meta platform represents.

In this dissertation we will use mainly the noun '*Facebook'* instead of '*Meta'* since in the general society it is the way in which it is most well-known. Although this highlight it will probably happen that the two names will be both used with the same meaning.

First of all, we are going to give a more specific definition of what data really are, and on what they differ from Big Data. We will try also to explain why they are so important and how, in this concern they are protected.

Afterwards we will outline a brief but still clear view of the history of Facebook and all the obstacles that it has faced in the last years. In order to understand this topic with a better knowledge we have decided to make a shortcut regarding the FCT Act, which is one of the most important reglementary paper on this topic. We will also perform and explain an analysis asking ourselves if Facebook really has market power.

The chapter that will follow is instead mainly focusing on privacy and we will try to explain what it is and how it is implemented in Facebook prospective.

After this excursus and the main explanation on how privacy is a predominant topic regarding sharing of information to other firms, we have decided to write another chapter on what really 'social control' is.

Explaining through different examples how it is implemented we can understand what is happening in the world we are living in. The main topics will be: geo localization, fake news and ads.

Social control is again a field that can be taken from different points of view. In this regard, our analysis will go into more detail on social control on concern of political thinking: how all data collected are used in order to perform political microtargeting and hence influence people. We will explain, in one of the last chapters why it differs so much from commercial microtargeting and what it really is.

On legal prospective many implementations are being made in the last years.

Since this is a “newborn” problematics, it is obvious that the first actions have been made in the recent past and many laws, created in order to take care of these happenings, are still developing.

But it is really important to understand how, in different countries and cultures, these laws have been developed during the years.

This is exactly what we will outline in the last chapter of our dissertation, with also the support of some real case examples.

Big Data

1.1 Understanding Big Data

"Big Data" is the buzzword of the decade.[1] All around us, from social media to lectures at university, everybody has heard at least once this word. Big Data are used in every field of today's market. Indeed, it is possible to speak about it in terms of a real Revolution, comparable to the French Revolution of 1789.

The rising phenomenon of collecting and elaborating them has impacted our society in one of the best ways.

Used in marketing (to predict and targeting profitable consumers) as well as in the social science sector (to study human interactions), the Big Data Revolution has helped in the research and then the discovery of vaccines for COVID-19.

As Andreas Weigend, ex chief of Amazon, has stated: today the entire world produces more data in one day then those which have been created by the entire humanity before the 2000 year.

Although their undeniable importance, nowadays this is one of the most discussed themes: the collection of so many informations could lead as well at an harmful impact of the privacy of subjects or other even worst consequences.

Thanks to its versality and so the application on so many fields, it's difficult to give a unique definition of what Big Data really are.

Indeed, at the beginning Big Data were seen as a mean to manage the cost of data management. Now, instead, firms focus way more on the costs of value creation potential.

Since 2011 our society started giving a prominent importance to this concept. Even though the sudden interest in this subject, it is a theme already broadly discussed and analyzed.

It is possible to track a short cut off of the many interpretations which this term has assumed in the past years.

The most known and taught definition was stated in 2001 in the Meta report. Now under the name of Gartner, it gave us the broad definition of the "three Vs" which stands for Variety,

[1] Contra Sanjeev Sardana, Big Data: It's Not a Buzzword, It's a Movement, FORBES (Nov. 20, 2013), http://www.forbes.com/sites/sanjeevsardana/2013/11/20/bigdata [https://perma.cc/9Y37- ZFT5]

Volume and Velocity. It is crucial to highlight that in this report they never talked about big data in an open manner. They indeed were just addressing the new trend which summarized an always bigger increase of the types of data collected, as well as an always bigger increase in the amount and speed at which these data were produced.

This definition has in the past years (2012) been implemented with the help of NIST (National Institute of Standards and Technology) and Gartner (consultancy firm).

It has been added a 4th , new, V: Veracity. It regards the characteristic of uncertainty of data.

Another definition was given by Oracle but it didn't imply Vs categorization. They stated that Big Data are nothing less than derivation of value from different kind of sources, which drive business decisions. This definition is focused on infrastructure technologies such as noSQL, HDFS and R and relational database. Unluckily it is not a very clear definition, and we don't have a wide explanation on when, actually, a data is a Big Data.

Intel, on the other hand, is the only firm that gives us a quantitative definition of Big Data: "Generating a median of 300 terabytes (TB) of data weekly"[2]. They, as for Oracle, think that the most important data can be taken from relational databases.

Although all these definitions are quite interesting to take into consideration, the one that should be more complete is the one that Microsoft provides us with.

"Big data is the term increasingly used to describe the process of applying serious computing power - the latest in machine learning and artificial intelligence - to seriously massive and of ten highly complex sets of information"[3] .

The motif of innovation in this case regards the fact that also artificial intelligence and machine learning are introduced.

Although the many definitions that we have just stated, the most important question regarding Big Data is just one: "Why they are so important?"

Indeed, we should highlight that is not the big data *per se* that are important, but the main aspect regards the action of analysis that there is behind.

Big data are at the basis of taking a decision in whenever field we are approaching. Summarizing: this incredible set of information, concatenated with the ability to perform a good analysis of this last subject increase, and not only of a small amount, the efficiency.

Corporations, in this way, can have a better view of their business and implement, as well, what is not as good as what is required.

[2] Intel Peer Research on Big Data Analysis

[3] The Big Bang: How the Big Data Explosion Is Changing the World - Microsoft UK EnterpriseInsights Blog - Site Home - MSDN Blogs.

Just to give few examples, here is reported a list of further implementations that can be implemented in different areas after having performed an analysis of data:

- By studying existing log (a technical world for expressing the term of "lines" of files), in the field of technologies, there could be an improvement in the security systems
- Enhancing costumers' satisfaction by customizing services
- Thanks to social media content, it's possible to improve services and products following the request of people
- Delay of online fraud
- Risk assessment in the financial market
- Etc.

This trend has the power to lead a revolution in the concern of how to do research, as well as marketing and innovation. Actually, it is already the case!
Many firms, like for example Ford, analyze Facebook's posts in order to understand what their customers really want and need. This is already a big change from the past.
With this, we can say that now we are talking about the importance of 'understanding data' and no more only about the importance of Big Data in general.

Understanding Big Data is not as simple as many can think.
It is of fundamental importance that knowledge regarding all the practices is shared and studied.
For this reason, people that work on this have a specific name and have signed the beginning of a new profession, which has been stated as the 'sexiest job of the 21st century' by the chief economist of Google, Hal Varina, and their name is: Data Scientist.
Big Data have many challenges but, unluckily, also the finding and consequently hiring of IT specialists is one of them.
According to a McKinsey's study there will be the need of more than 190 000 workers with analytical experience and 1.5 million data managers only in USA.
Finding qualified people for such a new and innovative job is not easy at all. Old generation, with experience, don't always have enough competences to accomplish the required tasks.
And the new working force that is being established is not enough to answer the demand.
For this reason, many incentives are being implemented in order to let new generation study STEAM subjects.

Moving a little bit further in the understanding of Big Data, we should take into consideration that we are not talking anymore about gigabytes unit of measure, but the quantity of data run is of the quantity of yottabytes.

As we know, the main issue of Big Data is the quantity: the number of data to be processed is huge.

Of course, this huge amount of data affects the process of collection that is before the analysis.

Now we want to put some light on the concept of collection and selection of Big Data.

Since now we have always talked about taking information but never how this action should be performed, it's time to go a little bit further on it.

First of all, we should highlight the fact that data can come from different source: either internal to the organization that is performing the analysis, either external to them.

Of course, it takes into consideration many kind of inputs: videos, pictures, data and different types of platforms (e.g. Facebook; Twitter; Instagram, etc.).

Up until 2009 the process of collecting data was almost standardized: databases were the basis of the businesses' processes; operational data store supported the operational reporting; and enterprise data warehouses (EDWs) stranded for implementing operation and strategic decision making.

Nowadays, since the aim is to understand what data tell us and to forecast a future threshold, the Apache Hadoop Open Source project is essential.

This project provides software for reliable, scalable and distributed dataset. Its function is to provide the best solution for processing the big amount of data that have to be analyzed.

It has been designed to scale up from a single server to many other machines. Its ability is to deal in a great way with failure and application layer.

This project is innovative and a pioneer in its field. It is for this reason that it represents in a perfect way the answer at many questions of the last years.

From what we have just understood, technology implementation is fundamental to a successful handling of data.

Since the characteristics of Big Data, we can clearly distinguish them from normal data processing on many dimensions: flexibility; speed of decision making; processing Complexity; data Structure: structured and unstructured; concurrency.

We can think about it in terms of two teams: the firm and the IT.

They should collaborate in order to reach their main goal: business implementation and success.

To do so, the IT should try to give the best tools to the business.

As we were saying: Apache Hadoop Open Source project is the answer at this urgent request.

Thanks to this project, not only the speed and all the other function of Big Data are fully taken into consideration, but it enables data scientists to find a usefulness in data that before were considered without any function.

Apache Hadoop has two main subprojects:

- MapReduce: is able to assign workloads across thousands of nodes. It basically splits works into smaller clusters.
- Hadoop Distributed File System (HDFS): it spans all the nodes to in a Hadoop cluster. It is needed in order to store data. It assumes that nodes will fail so it achieves reliability by replacing data across multiple nodes.

Now that we have given a brother explanation of what Big Data are and why they are so important, we can understand in which extension the topic is linked to the topic we are talking about.

Collection and analysis of these information are at the basis of how Platforms like Facebook works and on what they really implement their business.

In the following paragraph we are going to understand which laws rule the world we have just quoted and how they have been developed.

1.2 Legal implementation on Big Data

Big data and their analysis are quiet a complex and extensive field. Since now we have just underlined how they are collected and processed, it’s time to give a deeper look at the legal implementation of these last one.

Everybody knows that: ‘Law does not know ignorance’.

For this reason is essential to understand under which aspects Big Data, or more specifically, the collection of Big Data can be processed in the limits of the law.

It is not with exaggeration that we can say that institutions see us as an agglomerate of data, nothing more.

As professor Kathleen Sullivan stated: ‘Our biographies are etched in the ones and zeros we leave behind in daily digital transactions’[4].

[4] Kathleen M. Sullivan, ‘Under a Watchful Eye: Incursions on Personal Privacy’ in Richard C Leone and Gregory Anrig (eds), The War on Our Freedoms: Civil Liberties in an Age of Terrorism (The Century Foundation, New York 2003) 128, 131.

Since we are basically the physical version of Big Data, and everybody wants to be “safe” we can now understand how important the protection of these information are.

Big Data developed a really big challenge for their protection from two points of view: both processors and regulations.

Broadly speaking, EU regulations (but similarly to every other country) are based on three concepts: Notice; Choice; & Consent.

Despite the effort that institutions are putting in this project, and the fact that in this paper we are going largely to criticize their behaviors, we should also highlight consumers ’attitudes since they are not so justified as one can think.

Indeed, people ignore notices as well as choices and undervalue their possibility to give consensus.

The main issue is that a lot of people seems to be scared of the possibility that enterprises put their hands on their data, but actually they don’t take any action in order to protect themselves. Usually they don’t even read the terms and conditions: they just accept all of them.

From this point of view we can consider data – Big Data- as the new currency of 21st century. People provide their information in exchange of ‘free’ use of platforms.

So, are these free app/platforms really without charge? It is a question whose answer is easy to find.

The most though decision regarding privacy regards the standard under which they are established.

The 1980 OECD Guidelines have also today a great impact on data protection laws. Although they are still applicable, they are from a completely different era since they have been created at the end of the last century. The world has changed a lot since that time and also the way people think has completely developed.

Limits regarding how to deal with Big Data are the biggest issue that nowadays we are facing in this concern. There are a lot of contradictions regarding where the right stands.

Many questions arise when ethics is involved:

1. What can be considered lawful regarding taking information of a person?
2. Where these laws are enforceable? Do they have effect on terrorisms’ actions?
3. Is there a limit in personal consent?
4. What means the right to be forgotten? When something is really forget?
5. Which should be the role of governments in these field? How should they behave?

The problem of this is that, as everybody can imagine, it’s a really extended field, where a good choice and a bad choice is not defined. We lay in a grey area which is hard to hide.

Taking decision and understanding which the right action is to undertake is one of the most difficult things that has been faced by institutions.

Was hence important to set four high level principles that must be there in order to protect data. The following information have been published on a paper about Big Data Ethics by Neil M. Richards and Jonathan King.

Our society is in strong need of ethical parameters in order to understand the present. These four assumptions have the aim to peruse this job.

As first one we have: 'privacy must be recognized as information rule'.

Is crucial that the concept of privacy is well understood by everybody. With this last term we want to identify not only physical person but also legal one. Also companies and government institutions should start having care of this concept.

The second pillar is the following: 'Share private information must remain "confidential"'.

People think that after an information has been shared it must not be longer confidential. This is not true at all. It takes the name of binary notion.

This is a quiet dangerous pattern to undertake since it can destroy the trust that people have one for the others. Furthermore this information, today, are protected by regulations and so we should not have fear.

Third: Big Data must be transparent.

Transparency can go against abuses that can be undertaken by institutions. It also helps building trust in people in the concerns of government that collect these data.

Analyzing data and then sharing the results is a great way to establish a connection between the two figures involved (analyzers-instructions and analyzed-people) and can help the development of our society.

Forth, and maybe the most important: Big Data have a huge impact on people's identity and compromise it.

Although many individuals still have issues in admitting it, collection of data has a strong impact on their lives. An impact that, since most of the time the collection is performed in a hidden way, is not visible.

In this way is easy to affect behaviors and perform a total surveillance of lives.

From many point of view is scary how much we are influenced by factors that we don't even control?

But would it really different if we won't live in such a society?

We fell again in the grey area where there is not a good and a bad: everything is just up to the individuals' way of thinking.

For all what we have just said, we can conclude that regulations do not regard strictly Big Data *per se* but privacy, which is a topic we will focus on in the next chapters. It makes a lot of sense in the concern of what we are going analyze after the topic we have just taken into consideration: privacy indeed is one, if not the number one issue we can say about which Facebook and all other platforms that are used to perform social control have problems about. It’s not just effective knot but it also regards ethics and how it must be implemented in all the decisions that people take.

Facebook Case

2.1 Facebook history

Facebook is a platform that can be considered the most important and innovative invention of the digital era.

After having "beaten" its powerful competitor Myspace, its growth has had an outcast increase.

There have always been complains regarding the interconnection between this platform, Big Data stored and privacy protection, as we already said in the first chapters.

In this section we are going to analyze in deep the story of Facebook and its interconnection with the department of the Federal Trade Commission (FTC) and its homologues in other part of the world (Section 2.3 and 2.4).

Everything started in the 2011, when the FTC received many complains from costumers but most of all from the Electronic Privacy Information Center.

Hence, after these reports, the FTC started investigating Facebook for unfair and deceptive behavior.

This prosecution was moved in the regard of how Facebook collected and used users' data. Which is considered to go against Section 5(a) del FTC Act: fair access from third part to data.

The main problem was in the regards of how easily data collected where shared with applications already installed on the phone of the user. There were a kind of flow of information pursued in the same phone.

And it was not all, because the information collected and shared were not belonged to the main person but they belonged also to the friends of the subject.

It also happened if the user restricted all the concessions.

Basically, Facebook was not observing the duties that it tooks: it was just implementing the profiling for a commercial scope.

Of course, in this concern, Facebook was playing the role of the good guy, who trick everybody letting others think that everything was fine, and they were following the rules.

We can distinguish between two types of data collected by Facebook:

1. Data shared by the user: e.g. political and religious orientation
2. Data regarding the activity of the user on the social media: e.g. types of friends, pages more searched and videos liked.

After this investigation the FTC implemented some measures in order to protect the user:

1. Avoid to give false testimony regarding privacy and personal data collected
2. Give clear information to users and explain well how and which data are collected
3. Data must be remitted to the user in case of quittance
4. Good treatment of the data

Although it could be seen as a good agreement, the fact that it was never implemented cannot be considered as a great solution.

As all the problems that are not solved in the right way, it comes up again in the 2014.

Facebook was, in this year, accused of manipulation of data in the sense that, after a deep analysis, they showed on the first page (the one that pop up as soon as the app is opened) some appropriate contents specifically for that user.

The 2014 was also the year in which Facebook bought the well-known app named WhatsApp.

Facebook didn't lose the chance to connect WhatsApps' profiles to Facebooks' ones: which was not an ethical move.

Although many complains took place the FCT in this case didn't take any action and they left everything unchanged from the Agreement of 2012. The timeline took us to the 2018.

This was not only significant year for Facebook but it was first of all the year of the implementation of the biometric scanning. Which, in this story, don't follow different path, but a distinction is anyway important to highlight.

In this case, in fact, Facebook started taking all the pictures of the users and tried to perform the biometric identification of these subjects.

Also in this case the FTC didn't take any action.

Is in this year, after few months of the complains regarding the biometric profiling, that the most known case regarding Facebook exploded: Cambridge Analytica scandal.

Summarizing the problem, it's possible to say that Cambridge Analytica (a British counsellor firm) collected data from all the Facebook's users and draw a psychological and behavioral profile.

It was way worst then anyone could have ever imagined and, just to specify, it went against the agreements of 2012.

This was discovered by the New York Times and the Guardian, two well know newspapers.

Probably moved more by obligations than ethical sense an investigation started in 2019.

The information discovered after this examination were so scary that no one could have ever imagined it.

More than 13 000 app have had access to users' data. Basically, Facebook sold all these data to almost everybody that required it.

The platform did not, at all, changed its behaviors.

On the contrary, they also get worst.

It is possible also to talk about a phenomenon called *grandfather right.*

It is nothing less than a concession of collection of data by some firms (until 2018). The permission was extended just for few. Could we imagine why?

Although there is no need to specify it, one of these companies, was of course Cambridge Analytica.

This phenomenon was connected with the selective enforcement. Which simplifying means: to let companies gain as many data as how much they allow Facebook to gain.

Facebook allow company to collect how many data as they want, as soon as they earn them.

We are now talking about surveillance: social surveillance. We are going to talk a little bit better about this topic in the following sections (Section 3.1). Although the importance and the gravity of the situation, the FTC continued to negotiate and not punish the platform.

We can't take in any consideration a punishment of the obligation to pay a fine of 5 billion, compared to the incomes that this platform has annually.

Here an ethical question comes up: is the collection and sharing of data implemented by Facebook, which has a social impact, good or bad for the humanity? It could also help to take control of not good behaviors, and can you imagine if it could discover and stop a terroristic attack?

As we already said at the end of the last chapter ethics plays a crucial role in this subject.

From what the FTC figured out after the Cambridge Analytica case; we can deduce that there were probably more benefits than disadvantages. Indeed, the Federal Trade Commission implemented just few changes to the Agreement stated in 2012, and a new settlement was established.

The topics that were highlighted and altered were: internal privacy; and extension of concessions of data procession.

This is the end of the story as far, but there are many factors that let us be able to think that the problem will go on for many more years in the next decades.

For this reason in the next part we are going to analyze how the antitrust law has been involved in this topic and how it has been developed.

2.2 FCT Act

In order to dive a little bit more into the understanding of this complex case, it’s important to understand who should try to take care of the data that are collected and that everyday more and more people want to obtain and elaborate.

Since we are talking about an American firm, we can understand that its first guarantors are the Americans’ institutions. In the last chapter (Section 5) we are going as well to see its implementation in other countries (Germany and Italy), since Facebook is a platform established worldwide, but for now our analysis is going to be performed on one of the most important Americans’ institutions.

As we introduced in the chapters before, in the regard of the case we are examining we can relate on the antitrust committees that are established in this country.

To go for a short throwback, we can summarize the story of the American’s antitrust law in the following two steps:

- 1890 – Sherman Act’s: the first implementation of competition policy in the US
- 1912 – Federal Trade Commission and Clayton Act: since the Sherman Act’s was not considered enough to stem the anticompetitive behaviors a new act, the Clayton Act, was established with new revaluations regarding as well mergers.

Thanks to Wilson, in 1914 was endorsed a further commission bill: the one that will take the name of Section 5 of the FTC Act.

This section regards the investigation of unfair competition in regards of the commercial field. For this reason, it is so relevant to the analysis which we are conducting, and it pops up so much in the investigations regarding the Facebook platform.

The difference between these three entities could be more clear if we specify the difference between the Sherman Act and the FTC Act.

The Sherman Act outlaws "every contract, combination, or conspiracy in restraint of trade," and any "monopolization, attempted monopolization, or conspiracy or combination to monopolize."

If a violation of the Sherman Act occurs, the Supreme court, has already stated that a violation of the FTC Act occurs as well.

Furthermore the FTC also reaches some practices that the Sherman Act does not reach.

Another and last difference is that the Federal Trade Commission is the only body that brings cases under the FTC Act.

The cases for the Clayton Act are completely different since, as we already highlighted before, it reaches some categories that the other two Treaty do not reach: e.g. mergers and interlocking directorates.

Another distinction that is useful to make is the one in the regards of the Antitrust Division of the Department of Justice (DOJ) and the Federal Trade Commission:
They both enforce the federal antitrust law: in some respect their authorities overlap, but in practice the two agencies complement each other;
FTC devotes most of its resources to certain segments of the economy: health care, pharmaceuticals, professional services, food, energy, and certain high-tech industries like computer technology and Internet services;
Indeed, before opening an investigation, the agencies consult with one another to avoid duplicating efforts;
Only the DOJ can obtain criminal sanctions;
The DOJ also has solo antitrust jurisdiction in certain industries, such as telecommunications, banks, railroads, and airlines.

For what concerns our analysis is important to highlight that with the Biden's government it has been appointed, as a head of the FTC, Lina Khan.
She became a public figure thanks to her article on the Yale Law Journal: "Amazon's Antitrust Paradox".
In this article she appointed and criticize the Amazon unfair behavior which goes against the antitrust law, since, she highlights, they are exploiting their competitive power.
Her judgment was not over Facebook but it is still one of the most important giants business that over exceed in terms of privacy and exploitation. It can really be compared to the main case we are taking into consideration, but furthermore with the social control which is the topic we are trying to study.
American antitrust law is, as we have noticed, a main payer of the turns that this subject has taken.

2.3 Facebook and Market Power

A question that arises quiet easily at this point is if Facebook has used all the data collected in order to increase its market power. We have, since now, addresses the problem from a theoretic point of view: taken information and tried to elaborate on them as we do with puzzles, it means taking pieces and trying to make them coincide. Now instead we want to put all the knowledge that we had in action. Only in this way we can have a fully overview of the topic.

Before going on is important to define the subject we are talking about and ask us a question: ‘What Market Power is?’.

If we rely on the economic definition, it is the ability to set the prices profitability above the marginal cost. Or it is the "extent to which firms can hold price above marginal costs, measured by the Lerner Index".

The Lerner index can be considered a direct measurement of market power, which is the difference between the prices and marginal costs over the prices. The index might range between 0 and 1, where 1 means that the firm has the maximum of market power. Although its usefulness there is a problem with this index: usually data regarding marginal cost are not available and so the index is not always applicable in the real life (firms are not willing to provide true data regarding their marginal cost).

The economic definition is uncontroversial, but from the legal point of view the definition is the position of economic strength which gave a firm the possibility to behave to an appreciable extent independently of its competitors, customers, and, ultimately, consumers"[5].

In the case of the economic definition, there is a reference to the prices, but in the legal definition there is a reference to independence.

With interdependence we mean interchangeability. Hence, the legal definition of market power relies on it: which products are in competition with respect to their interchangeability because of their features.

The main point in this concern is that, in general, we cannot ask if a firm has market power, but it is essential to locate it in a specific market and geographical area.

In order to understand if a firm has market power there are three steps to follow according to this definition:

1. Define a relevant antitrust market (market in which goods/services are in competition: set of producst and geographical area that exercise some competitive constraints on each other), which has also a geographical extension. We can add that for the US Supreme Court: “Two products are in the same market if they are reasonably interchangeable”.
2. Define a competitive scenario.
3. Understand which is the degrees of market power.

Also here a problem incurs: how can we define which products are in competition with others? Which the meter of decision?

[5] European Court of Justice

In this concern we cannot rely on the economic concept of different industries/markets.

To solve this issue is needed a clear methodology: SSNIP TEST.

It was introduced in the 80s by some economists and it seeks to identify the smallest market within which a hypothetical monopolist or cartel could impose a small but significant non-transitory increase in price and defines this as a relevant market. The threshold number is the 5%: if a monopolist or cartel could sustain a price increase of at least 5% for at least one year on, assuming that the terms of sale of all other products are held constant, without the costumers switch to another product, this firm has the power to raise prices (hence has a market power).

The next closest substitute is added, and the process is repeated until the point is reached where a hypothetical cartel or monopolist could profitably impose a 5% price increase.

The range of products or the geographic area so defined constitutes the relevant market.

More precisely, it is thus necessary to take into the proper account three components of the projected price increase:

1) Demand substitution: which products are substitutes in the eyes of consumers?
2) Supply substitution: which suppliers may offer substitutes in case of a SSNIP? (short run responses)
3) Potential competition: which suppliers may enter the market in the long run?

If one of these forces is not taken into account, the resulting market definition will be too narrow.

Therefore, product markets and geographic markets must be determined simultaneously and not consecutively.

From the ’90s onwards it has been widely used for antitrust purpose.

There have been studied as well other kind of methods to determine market power: qualitative and quantitate studies.

Qualitative studies encloses all the event studies (evidence from substitution realized in the past) and surveys (market investigations addresses to competitors and consumers, even if there is a risk of biased results between actual and future behaviors).

On the other hand qualitative studies refers to cross-price elasticity (provides a ranking of substitutes but not a precise relevant market), similarity of price levels, price correlations (measure the degree of interdependence of prices).

After all these definitions and explanation, we can come up to the point where we can ask ourselves how all these methods are implemented in the different countries of the world.

It is important to have a wider view of the topic. In this dissertation, as it was already possible to understand and it will become even more clear in the last chapter, we have decided to address the topic from different points of view since we believe that in order to understand something, studying and understanding how the same thing is done in different ways is the perfect path to improve the method that it has already used.

Taking information from other countries and elaborating on them enable us to ameliorate our techniques.

Is it good for the market to have big firms? “Big is bad” is the slogan underlying the antitrust enforcement, even though this bias has been reneged.

Firms, always try to set as a goal to gain the monopolistic position in order to gain as much profits as possible, but the law steps in and states that when a firm is in that position there might be some problems.

Is it good for the market to have goods to be sold at low prices or is it better for the institution to intervene? Who is better off if the firm sets low prices? It is difficult to distinguish between welfare-reducing conduct and aggressively pro-competitive actions. Of course, for the consumers is better, but it is not good for the competitors of the firm since it encourages predatory pricing (the pricing of goods or services at such a low level that other firms cannot compete and are forced to leave the market[6]).

These problems have been seen under different prospective through different countries and as well years.

As we already anticipated in what we have already said there is a huge difference between the way in which US looks at the problem, compared to ho it is seen by EU.

While in the past American case law under the Sherman Act expressed a wish to restrict the power of big firms in favor of smaller firms, in the current US antitrust law the policy goal of promotion of small business has been discredited because of its inefficiencies. Indeed, the possibility of charging monopoly prices is what attracts businesses acumen: it induces risk taking that produces innovation and economic growth.

In Europe we have the art102 of the Treaty on the Functioning of the European Union which is the European version of the Sherman Act. It describes which practices may represent an abuse, but even in this case it is not clear which practices imply market monopolization.

According to the Art102 any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, specifically, consist in: Directly or indirectly imposition of unfair purchase or selling prices or other unfair trading conditions; Limiting production, markets or technical development to the prejudice of consumers; Applying dissimilar conditions to equivalent

[6] Oxford Language Dictionary

transactions with other trading parties, thereby placing them at a competitive disadvantage; Making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

In the end the Sherman act and Art102 are pretty similar, beside one element: when a firm becomes dominant (e.g. when it acquires a monopolistic position or when it has market power?)

Within the EU, the dominant position is a position of special responsibility (like an elephant in a crystal shop): if you are in this position, pay particular attention to the strategy you implement in the market. In the praxis of European law, aggressive practices are permitted to competitors, but not to a dominant firm, which is exposed to a "special responsibility", which may become a "particularly onerous special obligation" for an undertaking which enjoys a position of "overwhelming dominance verging on monopoly". A firm in dominant position has the power to behave independently of its competitors and consumers.

Summarizing what we have just stated:

- Market power: power to influence the market price of a product
- Monopoly: condition by which the market is served only by one firm; a monopolist is the sole supplier (and price setter) of a good in a market.

Now is quite interesting to analyze how all the information have been applied to the Facebook case.

Can we say that Facebook has created a monopoly?

The first question that we have to answer regards the constancy of the phenomenon: does Facebook recursively collects data and sells them to third party? Is this action used in order to increase its market power?

Is quite easy to see that there is a remarkable difference between this case and the one that we have highlight it the other sections: we are not talking about prices, but about quality.

The exploitation of the privacy of data brings to a decreasing in the quality of the service.

This ends up in a damage caused by a distorted exercise of market power.

Although we have explained, we hope adequately, what is and how is implemented the SSNIP test in this specific case, where Facebook offers a completely gratis service, it does not help at all.

For this reason, for this analysis is considered way more useful the SSNDPP - a small, but significant, nontransitory decrease in privacy protection.

Where the guiding parameter would therefore be represented by the substitutability for users of the data protection gradient.

The main point is that in a product for which the price is equal to 0, it's better to consider advantages (seen as surplus) that costumers can have from that specific, in this case, platform. If one app has better privacy policy will the costumer choose this one, or he/she does not care and hence choose another one.

The probability of switching gives us the market power that this specific product has.

We can hence think about its market power talking in the regards of data collected (always in the limits of privacy and data protection).

Privacy is a non-price quality parameter of completion in free services like Facebook.

Hence, Facebook can be though as a company that for sure, even more after the acquisition of WhatsApp hold market power.

In the end the outcome that comes up is more astonishing then expected: is the antitrust that, due to these uncertain times could endure a dangerous under-enforcement.

The antitrust law is struggling also just in taking action against these media giants that, for the example of Facebook, count more than 2.5 billion of users.

At this juncture, although is every day more difficult to enforce some, but even more we should say right, action, we can state that at least, the fact that the antitrust is trying to take some action in the best choice.

It is not still enough, but at least privacy is taken a little bit more into consideration. In the next chapter we are going to make a wider study of abuse of the power that Facebook, in tis specific analysis but still every platform that perform social control, in concern of exactly users' privacy.

2.4 Facebook and the privacy of its users: abuses of power at the expenses of user privacy

We have already introduced the topic of this chapter, but now we are going to focused more on the concept of privacy and it's real meaning regarding, as always, the Facebook's behavior.

As everybody can see in everyday life, many websites have implemented the Facebook 'like' to let users able to share their consensus and let *others* know what they appreciate the most.

Many times, users do not realize that in the middle of that *others* there is as well the platform itself, that stores data and then sells them.

Indeed, this tool is used to place cookies on the users' computers. We have to understand that cookies are nothing less than instruments used in order to take trace of users' behaviors and research.

Now that we have a little bit elaborate on that, can you imagine how many things Facebook can do with just one of your likes?

We have already explained how governments are trying to protect these episodes and we have, as well, tried to give an explanation regarding the ethic that there is behind this project (Section 1.2 and 2.2).

Since the story we already talked about Facebook and its relationships with data protection (Section 1.2), what can we think about its relationship with privacy? (Which in the end is nothing less than a more specific subgroup of data protection). What can mean the word 'privacy' for a platform like Facebook?

In order to define privacy we should, first of all, distinguish it from data protection.

They are two different things according to the Chart of Fundamental Rights:

- Privacy concerns raised when people started moving from the countryside to the cities. In the past the privacy problem was related, for example, to the fact that people could look into other people's windows: privacy was basically the right to be left alone.
- Data protection is the right to control the data concerning us. Hence is the right to control analogical and digital identities entirely.[7]

An important aspect of all this story is that we can also think about data as valuable objects.

We can have different kinds of data that companies would probably be 'happy' to pay: we do not have only names or mobile phone numbers, but also data regarding our interests in commercial attitude for example how much we are willing to pay for a product.

The only problem is that people do not actually care about their data.

Although they really spend a lot of time trying to safeguard them, in the end they do not value their privacy.

We are not able to provide a value to all the data that we disclose: we attach a value of 1$ to the disclosure of an information, then the value of our privacy is equal to 1$?

They are different concepts actually.

We have seen that there is a difference on legal ground between privacy and protection of personal data. This example shows that we are not able to provide a value for our information. We are basically paying with our personal data, without having any knowledge of the actual value that they have for firms.

[7] Sweeney, 2002

We think that we are using some services for free, but we are actually paying through our information (data).

Regarding data that are subject to data protection we can find different kind.
First of all we can have personal data which are data that are able to identify a natural person, so called ‘data subject’. They are all these data concerning our habits, lifestyle, personal relationships and so on;
Then there are sensitive data which instead are data that have a specific value (e.g. sexual life, political opinion and etc.).
Finally we can find the category of online data: with the development of new technologies categories of data have increased drastically (e.g. IP address, localization data, cookies, etc.)
Although we have explained quiet deeply this topic (section 2.4), we did not already asked the most important questions: Why should we protect privacy or data protection?

1. Because individuals may be associated with profiles that condition their behaviors;
2. Because those profiles could be wrong;
3. Because those profiles may reveal some details that individuals would prefer to hide or that individuals do not even know.

Among the Western countries there is a general consensus on the fundamental principles and basic rules that act as the nucleus of the different national laws on the protection of personal data.
Which are the problems on the legal grounds hence?
The problems are the same and complementary to the competition ones that we have stated in the earlier chapters. With regards to personal data, we have different laws according to the geographical area.
The international principles that stand in this concern are: substantive principles (regarding the processing of data) and procedural principles.

- Fair information practice principles (1970s) are basically implemented everywhere. They were developed by the US FTC in response to the growing use of automated data systems. They are a mixture of substantive and procedural principles.
- OECD privacy guidelines (1980): do not have a binding rule and only provide a rough outline.

There are huge differences among the most important and most developed economic areas: for example, if we consider the US as the counterpart of the EU, we can see different approached of the data protection (to have a wider view you can give a look at Section 2.3).

Regarding national law there are two main models:

- Sectorial Approach
- Omnibus Approach

We can conclude that in the US the protection of privacy and data is a sectorial one. There is not an omnibus legislation, but there are sectorial approaches according to the business and industrial sectors.

It is not possible to have a general overview of the rules that are enforced.

On the other hand, within the European Union, the approach is based on one piece of legislation at the international level (which has been enacted in 1995).

Later on, in 2016, the regulation of data protection (GDPR) was enacted.

Today the directive 95/46 is no more in place, it was replaced by the Regulation 2016/279 and it is applied in all Member States.

The first rule was the directive 95 (Person and attention to personal data), then in 1996 the law n.675 was authorized.

The Italian law was enacted one year after the directive. The problem is that this rule was at odds with the directive under many aspects. Italy had to enact a law on the protection of data to enter in to the Schengen Area. For this reason the Italian Parliament enacted a decree in 2003, but in 2016 the GDPR was enforced.

Nowadays this is the rule that our country has to refer to, even though another degree of the same decree was introduced in 2018 to master on some concepts. We are going to see the exact procedure in the Section 5.3.

The main topics on which the GDPR elaborate on are different.

First of all, it states that processing must be lawful and transparent.

Data have to be collected for a specific and legitimate purposes and uses. It is not possible to process data for a future service.

Only data that are adequate and relevant to the purpose can be stored. It is not possible to process data that are not specifically necessary to the fulfillment of the purposes (data minimization).

Data have also to be accurate, meaning that data have to be kept up to date.

Finally, it is important the integrity and confidentiality of data: it should not be possible for hacker to steal data. Data have to be processed in a manner that ensures appropriate security Legislation has been trying to lift the level of protection through technical means (encryption etc.).

Anyway, the GDPR applies only if some prerequisite are applicable:

- The processing of personal data is carried out by a controller established within the EU, that is by a person who performs an economic activity also within the boundaries of the European Union;
- Or, the processing of personal data is carried out by someone who is settled external to the European Union but the activity is related to someone living in the EU or the PD takes place within the Union.

Now that we have explained how privacy and data protection are implement in the different countries of the world, we can talk about the antitrust privacy dilemma, which is at the base of the impossibility to find a right balance between increasing privacy protection or decreasing it. There are some cases where is required a more concession and others in which, instead, a restriction is needed.

In other words, user privacy can decrease or increase as the result of alleged anticompetitive practices.

The main problem that this analysis brings with itself is the fact that in a world like ours, where everything is based on collection of data, increasing a protection of data can lead to a lower number of data collected which will flow into an adverse effect on the ICT economy value chain.

This is nothing less than a tradeoff between consumer welfare and business welfare.

We should take in consideration also the fact that less data collected can also bring to less protection against for example terrorisms or other kind of harmful actions.

On the other hand, this can also bring to some positive effects: business can finally meet their customers' needs; reduction of compliance costs; and in parallel enables firms to be more competitive.

As everything in life: there is not a completely good thing and a perfectly bad choice.

Is everything subjective and must be applied to the specific case that is facing at that time.

It is just a grey area.

From this argumentation we can deduce easily that there could be two possible outcomes from this story: a pro-competitive strategy or an anti-competitive strategy.

In data-driven markets, as we have already said, data are considered as sources of market power.

In this specific case, increase or decrease the possibility to collect data makes a great difference.

In the Case of Facebook in Germany (Section 5.2), authorities have stated that a decrease in privacy protection can just harm the final consumers, so it's not a good idea at all.

On the other hand, an increase in data protection can be cause of a monopoly, since it would exclude competitors.

In this concern hence is fundamental to observe if privacy is a price value parameter or non.
This is linked to the fact that if the parameter is quantifiable then it is objectively, meanwhile the other is just up to the subjectivity of the person who is experiencing it.
If the parameter is subjective it could have a bad impact on the implementation of antitrust law that has to be enforced.
In order to solve this problem, there must be used an objective point.
From this we can understand that the analytical framework requires a two-step process:
First of all it must be checked that the strategy of protection of data complies with data protection law; therefore there must be checked that the strategy is as well comply with competition law.

It can have four different scenarios:

1. Non-compliance with data protection laws and non- compliance with competition laws;
2. Non-compliance with data protection laws and compliance with competition laws;
3. Compliance with data protection laws and non- compliance with competition laws; and
4. Compliance with data protection laws and compliance with competition laws.

Now that we have examinate all the possible implication of privacy and how it should be protected, we can go on with one of the main topics of this paper.
It means that since privacy, as we have understood, is a really important topic in our life but not many people know its value, government and institution have taken advantage of it and nowadays are influencing are life, implementing a sort of social control, through the use of platforms and innovative technologies.
It is difficult to see in a critical way, but even more difficult to analyze under an objective point of view, but we have tried our best.

Social Control through platforms

We are lining in the 21st century and it is a world full of technologies but most of all social media.

These app rule our life from the early morning when we woke up, until we lay down again in the bad.

Partner the fact that they are extremely useful, and they allow us to do whatever we want in real time, they have become an indispensable item in our life.

They have enabled the human species to reach its million-dollar goal: give the possibility to everybody to have the chance to express him/herself.

If we think about it in this term, we can conclude that every app has its own function and influence our behavior under different aspects: Facebook not only allows everyone to say everything, but it knows what everyone says; Google decides how to tell us what we want to know and keeps track of everything we've been kind of interested in; Amazon tells us what to have, lets us have it instantly, and keeps track of all that too.

The point is not which app creates the profile of the user but is that they create a profile which probably is similar to the person they are trying to profile and are able to understand its action and influence him/her in his/her decisions.

Somebody has also arrived to stated that Google knows people better then how people know themselves.

In this chapter we are going to focus on three main topics that are at the base of the social control that is implemented by social media.

But first of all, let me introduce the topic with a fairytale:

<< Not long ago, in a distance world, there exists a system of federal publishers. They were trying to rule as many users as possible. Archaeologists would have called this prehistoric era web 1.0. Users, for some time, were happy, until the day they discovered that they too could easily become publishers and form their own communities and kingdoms. They thus created a new land in which the contents were democratic and where each user could become their own king. The new sites soon allowed users to publish their royal decrees (blogs), vote for content, find old friends, become influencers, have followers and in some cases become even more

powerful than the old publishers. Users called this new Utopia web 2.0. Welcome to the Social web "[8]>>

Now that we have understood how it worked in the past and what brought us to the point we are today, it's important to understand which consequences are going to be there.

Let's examine what the next Sections will talk about. First of all we are going to study what geo localization, a thing that appears such a simple tool that we use every day just to let our parents, friends and partners know where we are, represents in reality.

Later on, we are going to talk about a new field: Machine Learning. To explain in a clearer way the concept we have decided to use a real-life example that was implemented by some students.

In Section 3.3 we take into consideration what our brain is bombed every day with without us to be aware of: ads. We are going to explain how they really control and govern our minds.

In the last section instead, we have implemented a new phenomenon that only in the last years have appeared on social network. We are talking about fake news and its implementation with as well its dangers.

Let's dive in this fascinating and for sure new world.

3.1 Geo localization

The big change that has taken place in the ICT has strongly influence the structure of our society, also affecting the way in which we are all checked and in which power is built (who has power nowadays? Governments or Firms?).

Not by chance our society has been named as Network Society.[9]

Although it could be seen as something that happens only in movies, companies implement geo localization of people for real.

It is used in order to see and understand with who people connect, hang out and/or just spend time.

Geo localization means that a machine identifies and report the geographical location of a user, trough the position of a phone in most of the cases or of other technological tools.

[8] F. Mini, *Social Media. Introduction*, in R. Ford, J. Wiederman (edited by), *Internet Case Study Book*, Taschen, 2010, 232

[9] Castells (1996)

Platforms like Facebook, WhatsApp as well as Instagram have had the possibility to master their research on their users thanks to the implementation of a geo localization.

In this way they have been as well able to increase their businesses through personalized advertising which enable them to show the right product to the right person, increasing the possibility of selling that specific item.

In this way it easy to understand that these platforms have a great power on human minds. We are going to elaborate more on them in the following chapters.

How does a GPS work?

In order to better understand how the GPS system works, let's try briefly to describe it.

A GPS receiver processes signals received from some satellites on which the system is based and, subsequently, performs a series of calculations that allow to give the location of the terminal.

Once this information is obtained, through appropriate triangulations, is entered into the software to create the information required.

Each satellite sends a signal that is unique. Once it is the received the receivers reprocess the data and use it for positioning.

It looks more complicated than what actually is, but if you think about it for a second you can immediately see how many posts or stories are posted every day in which the user itself tag the place where he/she is.

Hence is relatively easy to deduce and store this information. Of course, we should also take into consideration that maybe, in order to enhance its reputation, a user can lie on where he/she is but let’s think this is just a remote case. Usually, people use automatic localization.

Is in this scenario takes the first steps no more the figure of the users, but of the *prosumer*, which is a user who is able to create contents and share info.

In this way it is possible to carry out horizontal control of the society: since it is possible to perform a sort of extrapolation from social media in general it could be considered a valuable tool to study society routines.

In other words: once posted/created the information shared with the community is no longer under the control of the prosumer and hance can be used to study in first place him/her and then the society in general.

The topic is easily likable to the concept of smart cities.

Singapore and many other cities in China are now called with this acronym.

A smart city is a normal city, as we all know, which has been implemented with further technologies whose aim is to make it more efficient.

Since 2011, China has undertaken a government-led “smart city campaign”.

This campaign started with cities classified as first-tier by the government such as Beijing and Shanghai and then it continued to second and third-tier cities which developed innovative smart city infrastructures.

On one hand, the smart city campaign in Singapore and China allowed to solve longstanding urban issues in terms of energy and natural resources demand. This approach has the potential to improve the quality of life of citizens. On the other hand, smart cities entail surveillance in terms of collection and analysis of large amounts of personal data.

Data generated within smart cities by users interacting with Wi-Fi, sensors and other kind of technology represent an important part of the data accumulated by the government. This data allows to formulate very sophisticated forms of surveillance and control which make it valuable for business and urban governance.

A society of control, which is able to access large amounts of personal data, can be represented through the paradigm of ankle bracelets, used to control home incarceration. These ankle bracelets give society a sense of safety as inmates are under control and they give inmates a sense of liberty as they are of out prison. But these safety and liberty are only apparent. Only the ones which do not have bracelets are really free.

However, the use of mechanisms relying on surveillance data may be desirable, especially in periods characterized by systemic risk such as the covid pandemic or in case of terrorism or cyberattacks.

Basically, people are selling their data in exchange of a more comfort life.

The implementation of these concepts in the European Countries have been regulated by the GDPR, as we have already seen in regards of privacy in the last chapter (Chapter 2, Section 2.3 and 2.4).

The GDPR contains provisions on both automated individual decision-making (making a decision by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain aspects about an individual).

Article 22 of the GDPR provides additional rules to protect individuals if the automated decision-making has legal or similarly significant effects on them.

According to the general rules for automated decision-making and profiling in the EU, automated decision-making may be carried out only if the decision is: necessary for the entry into or performance of a contract;
authorized by the Union or a member state law; based on the individual’s explicit consent.

Furthermore, we also have to check whether the processing falls under article 22. In that case the decision-maker/profiler must make sure to: give data subjects information about the processing; introduce simple ways to request human intervention and challenge a decision; carry out regular checks to make sure that the systems are working as intended.
Some limitations to the GDPR may be enacted by member states in certain contexts, for example when it is necessary to reconcile data protection rights with freedom of information and expression or to achieve related purposes.

This principle of sharing and transfer of contents as well as of all information, including personal information, represent the starting point of new control tools. It is, indeed, through this immense amount of data with a digital footprint (a trace of our activity in the cyberspace) that public and private institutions can extend their control over society, and it is for this reason that we have decide to analyze it.

3.2 Social control performed through Machine Learning (ML)

Is it really possible to influence social opinion, and hence having a social control on people, using machine learning?

First of all, let's understand what ML really is: Machine Learning is the science (and art) of programming computers so they can learn from data.
Machine Learning is great for different problems.
For example for issues for which existing solutions require a lot of fine-tuning or long lists of rules: one Machine Learning algorithm can often simplify code and perform better than the traditional approach.
It is also important for complex problems for which using a traditional approach yields no good solution: the best Machine Learning techniques can perhaps find a solution.
Fluctuating environments: a Machine Learning system can adapt to new data.
Getting insights about complex problems and large amounts of data.
Few examples of what MI can do are: classifying images, write articles, generating new images, forecast revenues and, something just few people have predicts, influence human thought.

Social Medias are increasingly populated by bots, which are often used to steer public opinion and control which content gets shown to users.

Bots are piece of software code that performs certain actions following the instructions of a highly specified algorithm.

Companies such as Cambridge Analytica (that we have seen in. Section 2.1) have used it to determine the outcome of political elections, and this has been done often in a quite significant way.

Bot influence has also been detected in the 2018 Italian general election and future elections are going to be increasingly affected by bots and artificial intelligence.

As with Cambridge Analytica many other experiments have been implemented. For example, a group of student decided to approach a very specific subproblem, which automatically generated realistic comments that are indistinguishable from human ones. In this specific case they decided to generate negative comments that can negatively affect the target individual.

This problem can be split in 3 steps:

1. First, they needed to collect a large dataset of comments from a social media platform;
2. Then, they had cleaned it and selected negative comments to train their model;
3. In the end they trained the model and generate new fake comments.

Their choose, for this experiment, as social media Facebook.

The first requirement was to have a large dataset of human generated comments.

Since there were not many goofs dataset in this concern they decided to build one. In order to do so we need to scrape Instagram. It was not the easiest thing to do, but in the end they were able to do so.

After having built the scraper, the other problem was how to trick Instagram into thinking that the traffic was coming from several different users and avoid the rate-limitation.

Since we were using the unauthenticated API they just need several IP addresses.

This was not a problem since they own a proxy company and could rely on their proprietary array of more than 100 4G proxies.

Doing so they were able to effectively create the most comprehensive public dataset to date.

In total they scraped more that 151 thousand comments from two leading Italian politicians.

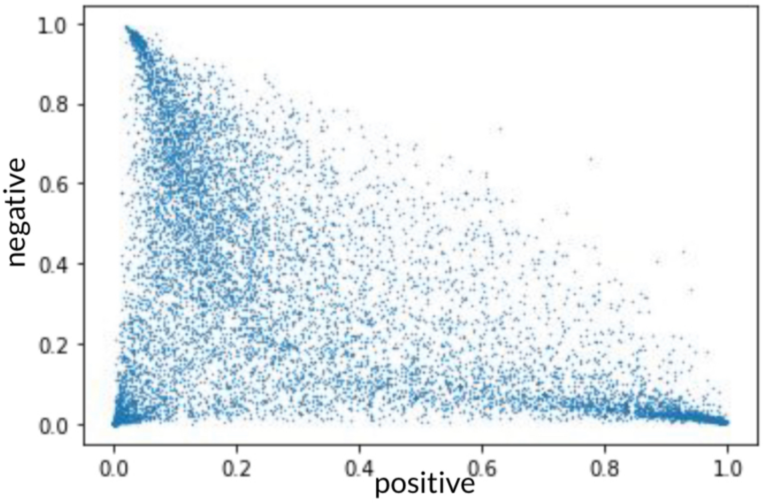
The second step was to clean the dataset and select negative comments. By performing a manual review of comments they were able to identify some uninteresting types of comments that could be easily dropped. These were: mentions, since all comments replies contain a mention; hashtags, emojis (since the model they were using was unable to process them), non-ascii chars in general, and URLs that come mainly from spam bots.

At this point they needed to extract negative comments from the dataset, in order to do so they perform a sentiment analysis.

The model that they were using was based on SentIta, a pre-trained sentiment analysis model for italian text. There were several limitations related with this approach, such as SentIta being trained on a relatively small dataset composed of reviews, but training from scratch was not an option since they could not manually label comments.
In order to train from scratch they should have manually labeled around 30 thousand comments which was not a feasible approach.

The model was composed of 2 dense layers, 1 convolutional layer and 2 bidirectional LSTM layers. In output they get two values, a positive score, and a negative score.
They then needed a way to classify the negative comments to prepare the training set for the RNN. Here they could see the scatterplot of a sample of 15k comments where the horizontal axis was the positive score of the comment and on the y-axis they have the negative score.

As we can see there are basically 3 regions that are more dense that correspond to the negative region, the neutral region and the positive region. But we need a way to cluster them.



IMG. 3.2 a

Afterwards, to make a good clustering they decideded to adopt KMeans Clustering, starting with 3 clusters. It must be said that the silhouette score is quite high (0,79) which means that the clusters are quite well separated.

The problem was that KMeans Clustering is not a method for prediction, because it was infeasible for them to run the clustering every time a new instance is added.

Thye needed to choose another method to actually work as a classifier, and for this reason they have chosen SVM.

So, they have split the 15k comments with labels in train and test sets in order to give as labels to the SVM the ones produced by KMeans.

Then, they have chosen the parameters C and the kernel by using GridSearch and they have obtained an accuracy of 99.68%, which must be interpreted not as a measure of error rate in classification but as a measure of how precisely the SVM follows the shape of the contours of the clusters given by the KMeans.

In other words, the error rate is primarily produced by KMeans and the SVM just tries to follow its results.

Now that they have a clean dataset of human-generated negative comments the last and most difficult step is text generation.

Their first idea was to use Transformers, Transformers are A Novel Neural Network Architecture for Language Understanding, introduced by Google Brain in 2017 with the famous paper “Attention is all you need”.

They overcome in clever ways the limitations imposed by Recurrent Neural Networks. RNNs are in fact very ineffective at text generation, even though some limitations can be partially overcome using LSTM. Their idea was to start with a pre trained model, such as GPT-2, and fine tune it to generate comments. Unfortunately, there is no pre-trained transformer model for Italian text generation.

Training from scratch is not feasible with their resources since they don’t have the bandwidth, storage, and most importantly computational power to do so. Cloud Renting is equally expensive and so we had to abandon their initial idea.

In the end, they therefore decided to use a Recurrent Neural Network.

They choose to base their project on textgenrnn, which is an implementation of the char-rnn model proposed by Andrej Karpathy (who is currently the Director of AI at Tesla). They trained the model with 10 epochs, they trained it on their GPU and took several hours to complete.

At epochs equal 10 there were significant overfitting issues, with output becoming total trash.

They were able to prevent overfitting by training with epochs equal to 5. This is due to their dataset being still relatively small, and were unable to train with more even when increasing dropout.

In the end they obtained a relatively good output, with main limitations being the size of the dataset and the badly trained sentiment analysis model that they have used.

From what this experiment has just showed us, is it really possible to implement technologies to have a social control on people.

It could be seen with a critical eye, but the truth is that the future is this and denying it won't stop it to happen.

A real-life example of how bot have been implemented regards the third US presidential debate between Hilary Clinton and Donald Trump.

It has been highlighted that bots have been used in order to increase or decrease (depends on which point you are looking at the episode) the consensus for one or the other candidate.

In this analysis have been analyzed more the 100 million tweets and it comes up that political bots posted:

- 36,1% of pro-Trump tweets
- 23.5% of pro-Clinton tweets

The journal the *Guardian* has reported a well that Trump shared and supported fake new about her competitor. It was not a fair behavior, but it was the right strategy to win the election.

This does not happen only in America, but is a worldwide phenomenon: Australian 2016 election; British election and so on.

We cannot do nothing more than accept that collection of Big Data and the implementation of political bot can really manipulate people way of thinking and that institution should just try to take care of public opinion.

3.3 Advertising & Social control

We have a little bit already anticipated the topic of this part, but now we are going to elaborate more on it: advertising.

As have been said by Christian Fuchs: Advertising are the primary source income source of mass media.

Indeed, social/mass media based most of their income on them and is also for this reason that they spend a lot of time trying to implement them in the best way.

Just to recall the example of geo localization stated in few chapters before: localizing customers has helped to send more accurate advertising and have a higher return of profits.

Although ads are seen as the major source of income, they can be considered as well a little bit biased.

In the sense that they arise as well some contradictions: on average, users click on few of them and so the message is not so effective as one can think.

This brings us to the conclusion that there could be an exaggeration of the real power that this tool has.

In the past, the best way to sell a product was to create an advertising on the television, and before the tv a great article on the newspaper would have catch the attention of most of the population.

But now, since we live in the consumism era and in a globalized world, few people take care about what pops up on the screen, and even fewer spend times reading the newspaper (there is always the tv news in the end…).

In a world where most of the people have whatever they want, is become more and more difficult to catch their attention.

For this reason, the means has changed and now almost everything is communicated through social media.

Facebook for example is not only a source of information (that can result also fake news sometimes), but it is also one of the biggest advertising companies, if not the biggest, in the entire world.

It is in the business of selling targeted ad space as a commodity and derive its revenues almost exclusively from targeted advertising.

The final outcome is an online advertising-users-spiral, which is a phenomenon that sees its birth within the world of newspaper, and now has shifted to the digital world.

An important example can be seen in the number that Facebook does in this field of concern: in 2013, Samsung invested more than $100 million in Fb’s ads.

For publishers, Facebook is a great source on which they can invest.

Since for many publishers revenues came up from how many clicks they are able to reach on their links/posts, it can be a life changer offering and posting their content on a platform with more than 2 billion of users.

Furthermore, using a platform like Facebook, will enable these content creator people to easily share posts with almost everybody and on different platforms as well, or the other way around (e.g. from a personal website to Facebook).

The implementation of ads can hance drastically change the life of an individual.

Although it could seem easy for us (we have just to plug in some links that are already ready for us in the platform), the behind the scenes is not so easy.

In other words, publishers are installing a Fakebook’s code into their website, which enables the platform to exploit the social plugin installed on other third-party website or platform to track and monitor users.

Is from this monitoring that the Facebook implement and adjusts its advertising strategies.

In order to calm down the publishers, the platform ensured that it won't never use the plugins for monitoring with the purpose of selling ads, but as we have seen it was not the case and Facebook did not maintain its promises.
A more even worst behavior conducted by Facebook was that the platform tracked the users also if they had performed the logout, which is of course a clear exploitation of market power.

Instead of changing its behavior, in 2014 Facebook officially codified its policy of using the plugin to track profiles.
Although it was already in action, now Facebook has the right and has also stated clearly that it is performing this kind of analysis.
Since this platform is both a commination network and a major advertiser, not such as firms like Amazon and Google, here we can talk about horizontal integration.
Publishers do not have to share information if they want to use the platform, but it is a condition that Facebook itself has set.

We can say that online advertising has four possible outcomes:

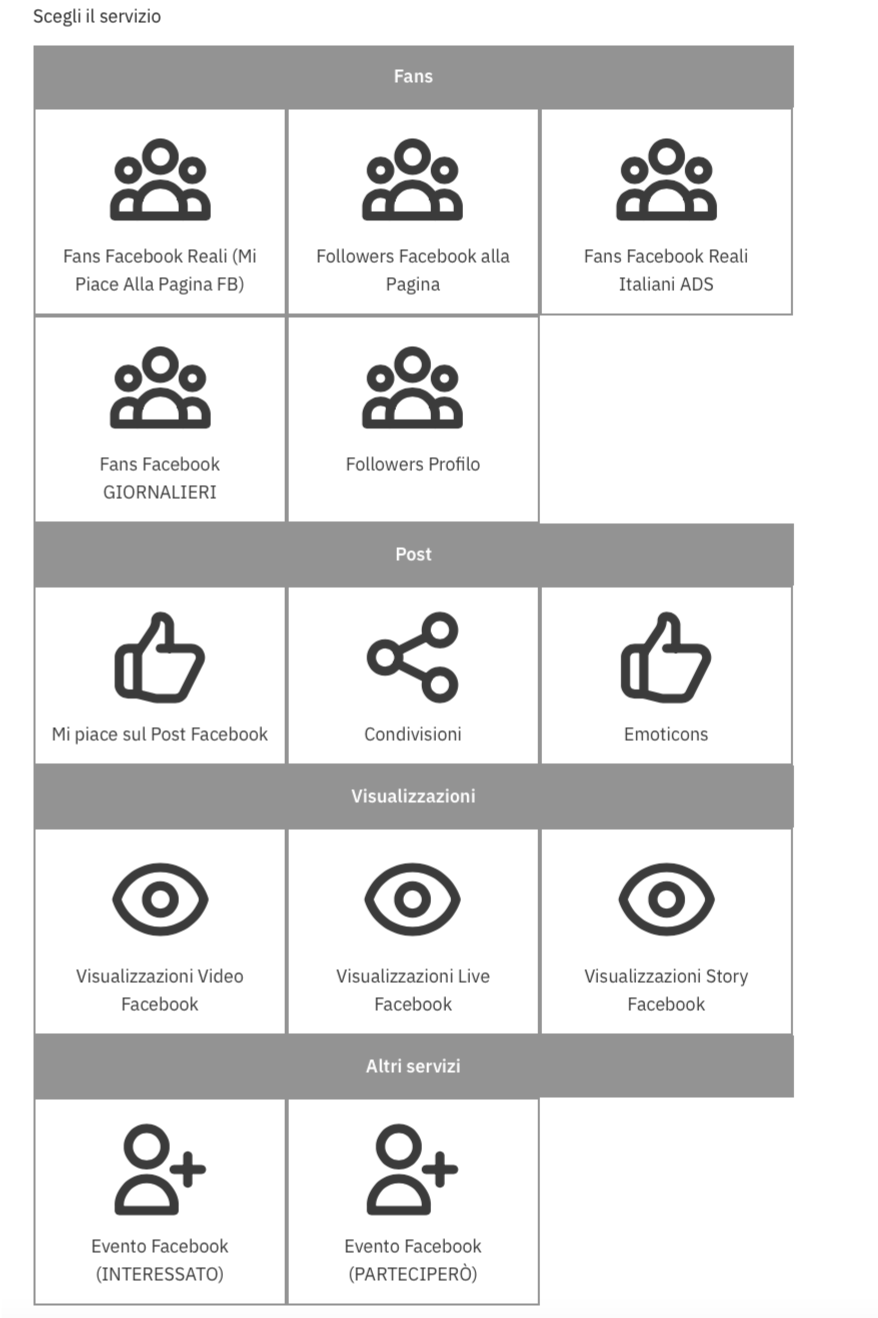
1. They allow the biggest firms, which have money to spend in advertising, to reach a slide of costumers way bigger than the smallest companies;
2. Normal content that is shared by firms slowly becomes more and more similar to what the company advertises and so there is a sense of lostness and a difficulty in discern what is what;
3. The advertising-users-spiral increases social media's power, encouraging the phenomenon that antitrust is always trying to avoid: monopoly;
4. Advertising means exploitation of audience labor: which is the characteristic because of which quality of social media services decreases.

Since internet has a decentralized and global architecture, sourcing is different in this case compare to the sourcing performed on, for example, TVs.
In any case, thanks to the fact that internet is a mass commination tool nowadays products can reach a larger a wider audience. And this is the main difference between broadcasting and computer networks.
Another important information to highlight is that in the online field, more is paid, more costumers can be reached. Basically, people can increase their audience just by paying.
They can buy likes, followers and so on.

In the following image (IMG 3.3 a) we can see how companies that sell this kind of product charge their customers.

SocialAds is an Italian company that sells “fans” on social media.

This is a short cut only for the platform of Facebook, but it can be done for many other platforms.



Scegli il servizio

Fans

- Fans Facebook Reali (Mi Piace Alla Pagina FB)
- Followers Facebook alla Pagina
- Fans Facebook Reali Italiani ADS
- Fans Facebook GIORNALIERI
- Followers Profilo

Post

- Mi piace sul Post Facebook
- Condivisioni
- Emoticons

Visualizzazioni

- Visualizzazioni Video Facebook
- Visualizzazioni Live Facebook
- Visualizzazioni Story Facebook

Altri servizi

- Evento Facebook (INTERESSATO)
- Evento Facebook (PARTECIPERÒ)

IMG. 3.3 a

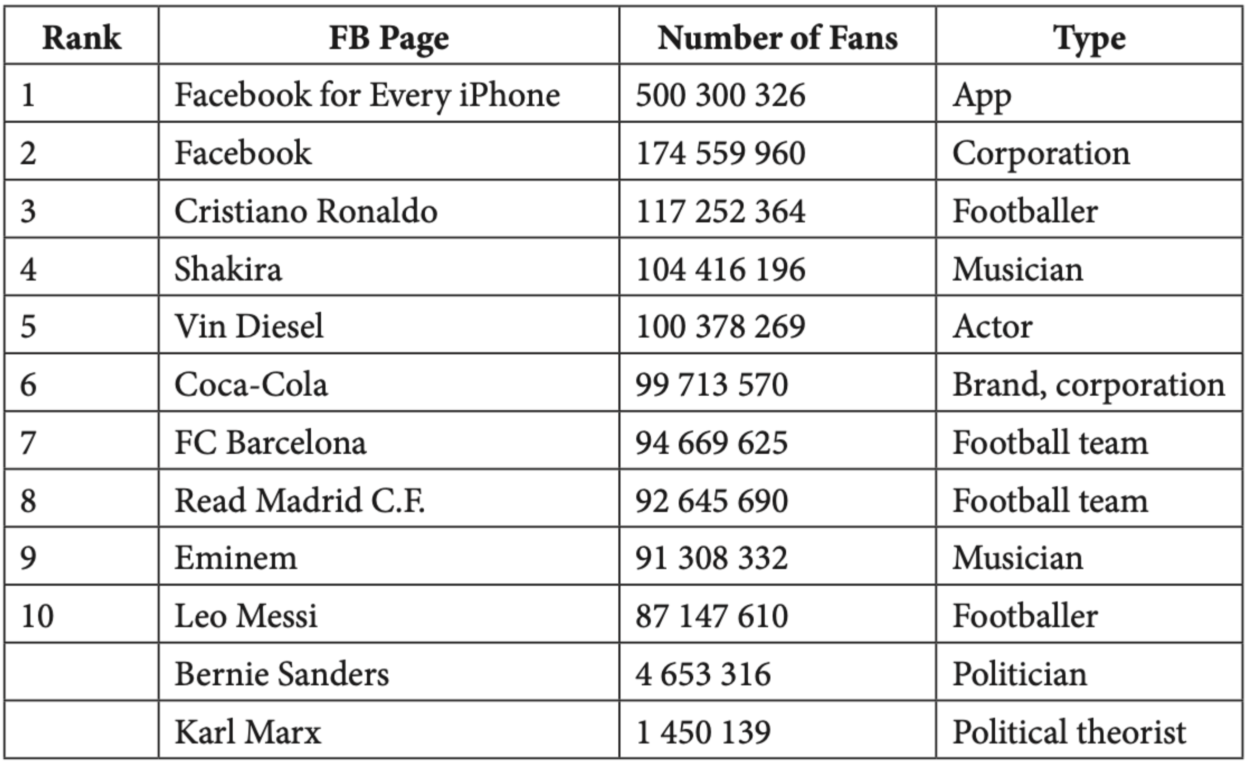
As we can see there are different options and different levels of ‘help’. Of course, services are charged increasingly due to what people wants.

Once a social profile has reached a certain level of follower and like, reputation hierarchical is triggered.

Other people will basically follow the profile just because is followed by many others. It is what happens also in real life in our society, just translated online.

And, has in society there is a division we can say in social classes.

Just an elite of people, dominate online, meanwhile the other are all spectators. In the following image (IMG 3.3 b) is reported the Facebook pages with the higher number of followers:



Rank	FB Page	Number of Fans	Type
1	Facebook for Every iPhone	500 300 326	App
2	Facebook	174 559 960	Corporation
3	Cristiano Ronaldo	117 252 364	Footballer
4	Shakira	104 416 196	Musician
5	Vin Diesel	100 378 269	Actor
6	Coca-Cola	99 713 570	Brand, corporation
7	FC Barcelona	94 669 625	Football team
8	Read Madrid C.F.	92 645 690	Football team
9	Eminem	91 308 332	Musician
10	Leo Messi	87 147 610	Footballer
	Bernie Sanders	4 653 316	Politician
	Karl Marx	1 450 139	Political theorist

IMG. 3.3 b

(The most popular pages on Facebook. Data source: https://www. socialbakers.com, http://www.facebook.com, accessed on 12 November, 2016.)

We can highlight, form this table, that the most followed people are not politics or institutions but singers and football player or team.

What can this mean?

There is a huge shift of values in the society of 21st century. Meanwhile before there was a high attention on what regulate the life of people, nowadays the last hit (song) or the score of a football game is more interesting than it. And we are actually excused for this behavior.

There is a set of social values that brings people to work more on what they actually like and less on high level topics. It is a way of thinking that characterize the 20s of our century. Tiktok is one of the most influencing platform and actually, with the content published, it is sharing this kind of way of living.

In this concern politics is marginalized and as we can see form numbers there is a huge gap between these categories.

Although their marginalization we can see, as we have already highlighted in the previous chapter, that bots play a very important role in online political communication.

Hence it is not just a matter of how many followers a page has, but also of how ads and others technological tools are implemented.

Following what just stated it has been developed a new model: propaganda model.

It is easy to implement since our society is divided in social classes, but it must also be adapted because of some characteristic of digital capitalism and digital media.

The Propaganda Model (PM) has some intrinsic characteristics that we are going to list hereunder:

- Focus on social media markets
- Targeted ads and content
- The online advertising-user-spiral increases social media's power
- Firms and entertainment dominate online ads
- Bots are the fulcrum
- Algorithmic amplification of online ideologies

The PM can be implemented in any social media nowadays since it follows the guidance lines of our society.

Now that we have talked about how advertising is used in order to perform social control, we can dive a little bit more into some kind of information that are shared on social media, and more than ever, influence human though and behavior.

3.4 Fake News

Since all these topics are strictly correlated, we have already talked a little bit about fake news and how they are used in order not only to achieve social control but also to enhance political carriers.

In this section we are going to give a definition to the term '*fake news'* and try to see what it really means in a political prospective.

We have already seen (Section 3.2) the case involving Clinton and Trump, but we didn't state what a fake news really is and when it could be considered so.

While we talk about fake news we talk about an environment which could be considered polluted, in the sense that is not clear.

As we could all imagine, there is not just one definition of this term: it lays, again, in that gray area that human species like to highlight so much.

This term has been started used from the 2016 onwards in America, basically after the election of Donald Trump as president of the USA.

For sure it was used also before his advent at the White House but is in these years that the term takes its political connotation.

The term 'fake news' ranges from the meaning of a notion that is shared through social media and is not true (basically approved by journalists and academics), to a polemic meaning meant to discredit "legacy" news media (supported by politicians).

Since the rise of a real phenomenon many other interpretations have been stated in the last years.

One of the most important says that they are: "news articles that are intentionally and verifiably false, and could mislead readers.". [10]

Other people feel that a fake news is just linked to the advent of internet and so is a problem of online disinformation.

Wardle in 2017, in an article focused on fake news, explicitly give us the different typology of mis- and disinformation that can occur since there is not just on type:

1. Satire or Parody: no intention to harm but has the potential to do so
2. Misleading Content: use of information to frame an issue or a person
3. Imposter content: genuine sources are impersonated
4. Manipulated content: when image or notions are manipulated in order to deceive
5. False Context: true content is shared with false contextual information
6. False Connection: headlines or captions do not support the content
7. Fabricated Content: content that is predominately false

There can be different kind of definition, and actually there are many more interpretations that could be given to this term, but the main point is that there two lines of thought: some people think that fake news are just part of a bigger group of disinformation and misinformation, while other think that; they are just the result of deception.

To summarize, while talking about fake news we can take many different objects under this meaning.

From wrong notions to misguided once to again invented information.

[10] Alcott and Gentzkow (2017, p. 213)

We do not know if it is such an easy thing to trace a line between when some news becomes a fake news or can be considered just a half-truth.

For example, when politicians try to impress their audience and so construct a real story all around the image that they want to share.

In this concern we can think about the duality of the fact that it could be seen as an ethical or non-ethical things to do (and this is just up to each individual- whatever he/she wants to think), We should not be astonished that there are entire courses about 'story telling' that are though in universities all around the world: they teach students how to "sell" (also in a figurative sense) a product, a story or a person as well.

We can take in consideration the Berlusconi case.

Silvio Berlusconi is a very well know Italian politician that has been President del Consiglio until 2013.

Thanks to the structure he gave to its social media he was able to reach a lot of consensuses.

Everything started in the late 80s of the last century: at that moment Berlusconi was just a powerful Italian entrepreneur but he was already sharing with an audience propagandistic message through, for example, the television.

In this way he was able to let himself and also his family be known by almost everybody.

It is important to highlight the fact that Berlusconi was the owner of a television network, and this could have helped him in the affirmation of his figure.

Connected to the fact that he was really able to have a strong influence on social media he also created ad hoc information in order to influence the perception that people had on his figure.

In addition to conventional communication tools, institutions and authorities have had the possibility to generating imperative speeches at the same time of sharing them through the use of new technologies.

A clear example concerns the exploitation of the news regarding the terrible earthquake that had hit L'Aquila in 2009.

It's terrible to say but politicians manipulated this catastrophe.

The calamity occurred during a delicate phase in the political life of Berlusconi. If he would have sent help and showed his contribution to the cause, for sure, his image would have had benefits from it.

It was exactly what he has done: Berlusconi and his ministers went multiple time to visit the tortured territory, taking pictures and trying to let people seeing their effort and concern about the cause.

Basically, they exploit it to make same sort of propaganda.

In this case media performed a double function: internal (on a national scale), aimed at making the event spectacular for the masses; and external (aimed at world power), with the aim of restoring international political credibility to Berlusconi.

Through the communication tools that Berlusconi implemented, he was able to perform media practices of vertical control and contributed to the definition of a space of power over which the government apparatus exercised its powers exclusively.

In this concern some aspects of his politics have been perceived as excuses to justify his goals. An example was the militarization of cities which instead was sold as a need of security of places that could risk further attacks.

At the same time, the media did not say nothing about the coercive control actions taken by the Civil Protection which avoided assemblies and leafleting.

What can we say at this point? Are all of them fake news? Are they not? Are they just news told under different prospective? Is the reality really manipulated or it is just that it has been told by a subjective point of view?

Unfortunately, we are not able to answer to this question, since a univocal answer does not exist, but at least now we know what happens behind the scenes.

This topic brings us to a new discovery: social media cannot control all the content that is published on their platforms. But do we really can believe that fake news implements social control?

It could be nice to see also the other side of the coin, where fake news are not considered as a threat.

People should not be scared to be socially controlled if they are sure about what they believe and support.

Here comes the difficulty: how to be sure that you have not been influenced?

Clarke Cooper, in his article titled ‘Deciding the Facebook question’, trys to answer this question, explaining that fake news are just a mirror of our inner self: they reflect what we think without limitations.

The World Wild Web (WWW) has been created with the idea that everybody could have shared its own opinions. It is with this excuse that the spread of fake news has been implemented.

Giving so much of freedom has also its consequences: everyone can put online garbage information.

We are falling again under a gray area, which is impossible to state if it is a good or bad development of our society.

It is for this reason that social media are unable to take things under control and probably they do not even want to do so.

Although their not will to limit people behaviors and thinking, there exist a working figure called *cleaners* who's job is to 'clean' the social media.

In Facebook there are almost 7500 people that perform this job, and they are hired from third party firms.

The main issue, if they decide to monitor post, regards how to categorize inappropriate posts, for the same reasons we explained before.

The Facebook app in fact knows everything and it also knows who says what. We are always controlled and monitored.

But the main problem is that we lost the power of governing our own data, and nobody asked us if they could do it. So we have been processed without having had any kind of process. Not very democratic for countries which state to be so.

The only solution that could be find lays on privacy protection, that we have already explained before.

We can conclude this chapter with an assumption that it will last until we do not know when: the main problem of people in these days of uncertainty is taking care of civic and social environment, which is not easy at all.

Political micro targeting

4.1 Political and Commercial micro targeting

Social networks, together with search engines and advertising companies have created, in the last years, a real ecosystem.

It has fundamentally changed the way people around the world use and receive information.

All companies and websites within the digital ecosystem compete to get the users' attention at the same time. Furthermore, they also affect every aspect of our society, from how we raise our children to the products we buy.

Before going in depth within this subject let's clarify a little bit more on what a digital ecosystem is.

What is an ecosystem? The biological concept that everybody knows has been applied to businesses. Different types of actors make the ecosystem what it really is. So we are not talking only about the people and the communities, but also about the technology providers. Whenever you want to address problems regarding not only the value generated for an actor, but the value generated for many other members of an ecosystem.

An ecosystem is a dynamic structure, it is not a hierarchy, not a formal contract between party and it is not a market.

Since we are talking about business ecosystems, we should also talk about ecosystem strategy implemented by a firm: the firm is aware to be part of a competitive ecosystem, to be either the focal firm or a complementor and its strategy is based in order to secure itself the right role in the competitive ecosystem.

In an ecosystem, the value cocreation is at the base of a good ecosystem and is also the only way to let it work in a proper way. It means that what each party is offering must be specialized, but it does not matter how much it is specialized, but how much it is co-specialized: something that combined with others's service will become beneficial to users. Basically actors share resources and capabilities to reach a common goal.

There exist three types of complementarities:

- Generic: there is no need for specific coordination (loans).
- Unique complementarities: emerge from co-dependencies between the resources and capabilities of ecosystem actors. Two actors that need each other, A can offer this service only if B is present.
- Supermodula complementarities: emerge as the value of one resource or capability increases when combined with others. If there are resources A and B, they might be

independent in the sense that A could be offered without B, but putting them together the value will increase.

Hence, ecosystems are just the conglomerate that rule our life.
Thanks to this the microtargeting firms are able, sometimes even better then us, to understand our personalities and our tastes.
Some of the microtargeting campaigns have been so powerful that people sometimes dream about it when they are asleep.
Microtargeting is one of the latest marketing techniques uses to promote businesses. It helps organizations identifying consumer behaviors and tastes. It has already had many different uses in the marketing world.

As we can remember (Section 3.4), Berlusconi, at the beginning of the 90s was the first Italian politicians that introduced what we can call modern marketing methods.
He was the first that appointed public surveys in order to value people's opinions. It is conveyed a sense of involvement never felt before in our country.
Furthermore he also created the tv advertising campaigns (we should remember that he was the owner of many tv channels).

Years passed by, and many things has changed in the last thirty years and now the focus (as we have already seen) is on data and their analysis.
Under this light, people are no more human being, but just interfaces from who they have to extrapolate information.
How this shifted happened? We can summarize it in three phases:

1) Microtargeting: it was based, at the early stage, on surveys performed also by going house to house asking questions. After the survey, data recorded were registered in a database (this idea was formulated by political parties that really seek this notions).
   The most important implementer country was the USA. Followed by the EU that, anyway is way behind America.
   A clear example is the '*Una storia italiana*' journal created by Berlusconi and distributed in the whole Italian territory.
   Although it was a sign of high maturity by our country, it represents as well the slowness of Italy compared with the other countries.

2) Digital boom: as the word says the digital has had a great impact on our life. In 2009, in the United Kingdom the expensed for online advertising excited the one for television ads.
   In the years the system has become even more complex with the introduction of social media.
   Until 2019 more the 50% of total digital cost were just for adverting.
   We do not know yet which impact has the digital had on democracy, but everybody is pretty sure that we are going to understand it very soon.
   In this phase, people are no more just numbers in a database, but they are actually interconnections.

3) Cambridge Analytica: the third and last stadio is represented by the firm about which we have already talked and explained a lot.
   It basically represents what advertising firms will be able to do in the future. They have been hence a projection of the next years.
   Their capability of deal with all kind of data and influence people in such a strong way is astonishing.
   By the way we have already explained also the ethical part of this story and we won't go on in repeating it.

As a tradeoff of this short introduction we can state that should be first aim of all subjects to take care of their information and to learn him/herself how to prevent these firm to perform a profiling of their personalities, although nowadays has become a really though aim (as we have explained in Section 1.2).

Although we have talked a lot about all its negative effects, we did not yet stated a definition of microtargeting.
It is a practice of collecting user data, including what they buy, their demographics, what they like and what they are most connected to.
Companies use this data to segment people into different groups for content or product marketing reasons.
The main purpose of microtargeting is to create a marketing strategy that delivers advertising to a specific type of people.
We can hance say that it predicts interests, influences, opinions and shopping habits based on behavioral, geographic, psychographic and demographic data of the user.
If you start thinking about it, you'll realize how true this is.

For example, if you search for the latest Lenovo laptops, Google will start showing you advertisements on different types of laptops (for more specific go to Section 3.3).

Facebook uses the same technique to determine which ads will pop up in your home. In general, it helps organizations or individuals to provide you with useful and relevant content, but this is not the only way in which you can think about it.

However, it provides you with incorrect or biased information, the only purpose that this firms have of which is to influence your decision.

Microtargeting aims to create a more comprehensive advertising strategy: it is basically an super plus level regarding ads.

The strategy is based on predictive analytics along with consumer data collected across multiple sources.

It is scientifically proven that campaigns that target a certain part of society are way more effective than unrelated advertisements.

They result in a better return on investment because they are more interesting, more compelling, and more relevant. More importantly, they also increase consumer engagement.

For example, people who love football are sure to have a keen interest in a football-related campaign.

On the other hand, the user will quickly lose interest in volleyball-related advertisements simply because he/she doesn't like it as a sport.

As a conclusion business can easily get to know most people interests, opinions, preferences, and habits just from their online browsing history or habits.

Now we can ask ourselves: Which is the extent of this phenomenon?

Recalling that the most important platforms for microtargeting are Facebook, Tweeter and YouTube and remembering that all the three of them have testified at the United States Congress for harmful Russian activity on their platforms during the 2016 presidential election, we can understand that the degree of importance is not so low.

The business model of these firms has three main components/objectives:

1) They want to maintain the users' attention for as much as time as possible.
   Here the home of Tweeter and Facebook plays a predominant role since they are always updated.
2) These firms want to collect as many data as possible in order to profile the users.
3) Furthermore, these firms develop digital algorithms for two main reasons: the first is to predict the type of content that keeps the user hooked to their network; the second function instead consist in showing only those ads with the content users are most likely

to click on. This practice is performed because in this way firms can reach optimal revenues.

These business model allow two categories of people to get the maximum from them: Politicians and Marketers.
Digital platforms that perform microtargeting hence show the user posts, images and videos that can capture their attention and then apply on their responses some algorithms that help them profiling the user.
Companies and firms, afterwards, can use this information to reach their marketing goals.
Both politicians and commercial entities use microtargeting, for this reason we can talk about two different types of this topic: political microtargeting; and commercial microtargeting.

Political microtargeting is believed to have played a crucial role in the US election that have seen Donald Trump become president of the United States of America in 2016. We have already talked a little bit of this while analyzing Fake News in Section 3.4.
Trump's Campaign Head Digital Strategist has stated often that they implemented this technique to communicate with people all over the State. They in fact used Facebook and Instagram to show the image of Trump that they want people to see.
Compared to Hilary Clinton, that used social media without microtargeting implementations, Trump also spent more than 150 million in targeted ads. This was the secret of his success.
Indeed, it was not the first time microtargeting was used in a political election.
Obama as well, in 2008, spent millions on a team made up by data scientists, database engineers and so on.
His team worked a lot for recreating a database of possible democratic voters.
This database included all information about voters based on their general interest, online and offline behaviors, and social media profiles. A real scanning of the population.
The team also used this data to come up with a comprehensive marketing strategy to target people in the best possible way.
Obama campaign was so successful that he was not only seen as a president, but as a friend.
Ads and competitions where people could have won a dinner with the future leader of the USA had a great impact on people thoughts.
It is impressive what institutions can make you think and believe.
At this point we can see the birth of a new figure: the spectator voter[11].

[11] Cristopher Cepernich. Le campagne elettorali al tempo della networked politics.

The political field is not seen as in the past. The politicians are indexed as performers that must show up their characteristics, meanwhile citizens have the role of just viewers.

The voters is hence passive in the whole process of the election: he/she listens, judges, sees but does not participate in an active way. This is the result of the tele-politics.

Now that we have talked about political microtargeting is the turn of commercial microtargeting, or what is called as well marketing microtargeting.

Just like in politics, marketers have been using this marketing technique for a long time and with good results.

The main principle is the same that we have explained before: taking information from like and dislike users put on posts, and understand their buying habits.

Afterward, the cluster of customers is divided into different groups and devise marketing strategies to target them based on their habits and behaviors.

In this concern we can talk about inbound marketing.

There have been developed five different stages of micro targeted inbound marketing:

1) Attract: drive the right kind of customers to the business. Basically, is about attracting the right audience;
2) Convert: the main point here is to crate engagement and monitor users' interaction;
3) Micro target: understand which kind of people are interacting between the current platform in use and setting up campaigns in order to do so;
4) Close: When you have all the information is the time to close;
5) Delight: keep and deliver constant updated about the information the providers has sold.

Just to specify with inbound marketing we mean a business methodology that attracts customers by creating valuable content and experiences explicitly for them.

Let's suppose that the main aim is, as for politicians, to understand the customer and trying to provide them with the ads that better fit them.

The first step is to identify actions and attributes of previous customers.

Next the main point is to collect all the data about the users (e.g. their age, location, purchasing power, education and income, etc.)

Then, it is better to booster the strategy by adding the research and collection of more information such as travel enthusiasts, gamers, pet owners, and TV show lovers.

They do not have to be difficult or main information, but it's enough that they are marginal.

Indeed, it is possible to attach any attributes we wish to segment your customers.

Nowadays we heard so many people saying that politics is just a matter of marketing.
This transformation is not due, in Luciano Floridi opinion, to a digitalization effect that has shifted politics, but because communication has raised to a higher level: the check and manage citizens.
Hence, in his reflection Floridi states, that:

- All the politicians (of all the democratic countries) are the effect of this transformation and not the cause. As we can see in the Darwin's world conception: the organism benefit from the change of the ecosystem, and not the other way around, so;
- There is a need of change if we want things to follow a better path. And we have to work on the communication system first of all

Although it is also important to identify as many attributes as possible. In this way it is possible, as well as, to overlap all of them and then create specified subgroups of a broader audience.
The result will be great: there will the possibility to build a large audience of potential customers. These are the customers who share buying habits and traits with people who have already purchased the products for which the research has been started.
Although it is possible to think that this advertising technique is based on the amount of data collected, it doesn't focus on quantity, but rather brings real, quality customers to the business. It also let us understand and predict which customers will be easier to influence.
Now that we have a micro-targeted audience, it's time to invest: it is possible to set aside some money from the marketing budget or spend it too.
It further helps to break into a niche market only if you can deliver relevant messages to the audience.
We should keep in mind that microtargeting is totally different from the spray and pray marketing mode.
'Spray and pray' is a method that consists of sending out mass numbers of generic outreach. It is basically advertising what the business does everywhere at every time and of course in microtargeting we do not want it and we do not need it.
It's a consumer first approach, exactly what is needed to personalize messages and develop personal connections with an audience tired of advertising.
Because this is exactly the issue: people are tired of advertising spread everywhere.
On the other hand, it is also possible to get your hands on big data by targeting a certain group of people. With these, we can use this data to create a personalized and comprehensive campaign that delivers relevant messages to your most loyal customers.

Is usually implemented a very known strategy to increase the possibility to have a better outcome: send messages to their favorite devices.

This is especially important if cross-device marketing campaigns are involved.

As we have already stated microtargeting has have positive feedbacks in recent years.

It is perhaps the most effective marketing medium in the digital world where it has become increasingly difficult to create a message that not only penetrates through the clutters, but also was specific with audience and forces/influenced them to also buy.

Some of the smartest companies in the world have realized that the only way to increase ROI is to increase the relevance of campaigns.

But the main problem was that businesses can't afford to spend so much money on unnecessary and unrelated marketing strategies. So microtargeting was the solution.

It is no more possible to just send personalized messages to a target audience.

In fact microtargeting allows to send messages to a certain group of people with similar needs, habits and traits.

It can really improve brand awareness, customer engagement and therefore sales.

Microtargeting is especially beneficial for direct sellers who focus on acquiring qualified leads to increase sales.

They can use the technique to send highly personalized and relevant emails to a small group of people who live in the same city and have similar habits, interests and needs.

They may also be of the same age group or work in the same industry. There are so many options.

So what should be taken in consideration while we talk about implementing microtargeting?

Here are seven essential factors to consider:

1) Focus on the relevance: take what is essential about costumers' profiles and send personalized messages.
2) Focus on the right cluster: it does not make sense to send a message to thousand and thoued of people when the right ones are just on hundred specific one. Just go for the people that will listen to you.
3) Multichannel campaign: spread the specified message through all the different social media. Do not use just one.
4) Know your aims: set an aim and work to reach it
5) Quality: this is the most important characteristic, do not loss it in the name of quantity.
6) Work on the satisfaction of the client: do not work just for the ROI.
7) Time: do not rush, it will not help the process.

The only main problem of microtargeting regards the spreading of fake news (Section 3.4), that is quite strong and easy to look at in a complex ecosystem like the one where this technique is implemented.

Unfortunately, ethics is not one of the main topics about which people think and discuss when implementing microtargeting.

Now that we have explained what political microtargeting is and its main difference with the commercial one we can go further in understanding what happens when this topic is applied to the world of IoT.

4.2 IoT: Internet of Things

In order to understand the impact that Data Collection has on social control we should also relate on one of the new most important development that technologies are undertaking: implementation of IoT.

IoT states for Internet of Things, sometimes referred to as Internet of Object.

We can summarize it as the way in which objects/things are technologized. We are trying, basically, to let everyday appliances (like fridges, lights, heaters, etc.) become smart.

A clear example of this can be a fridge that can communicate with the grocery shop, or also a smart watch.

Taking in consideration the last-mentioned device, we can think about how many things this object can actually record: consumers' steps, stairs climbed, activity performed, calories burnt, body temperature, etc.

This means that buying a smart watch the consumer does not only buy a normal watch.

This leads to tree main implications:

1. Consumer will engage in transactions with many different players (in terms of sales and contract law)
2. Each smart package will be different one from another since it depends on the frequency with which the consumer uses it
3. It's important to ask under which extent the quality of the personalization can transform in the assessment of the product?

The main point of this section is to point out the fact that these devices collect and process a lot of information and hence they target behaviors of consumers.

This development of devices leads to a change, not only with regard to the relationship that companies have with their costumers but also on how the companies approach them. Since they have access to such a bunch of information companies have the opportunity to learn a lot about their buyers.

Cisco has conducted a prompt analysis in this concern: it has been discovered that in 2020 fifty billion devices were connected to internet. Can you imagine how many information they have recorded?

This data means that there are almost 7 connected devices per person.

Furthermore, is important to highlight the fact that the quality of data collected by IoT are of a really high standard since they collect information about daily life of the consumer: so it's quality data.

Profiling performed in this way means that there is a shift from mass communication to a more tailored method (we have introduced this topic in section 3.1 regarding the social control performed in Smart Cities). Indeed it will be introduced a more personalized relationship between the two parties: consumer and provider. Of course, profiling is not only performed by IoT devices, but it can be stated, since the nature of the information collected that IoT offers great opportunities of profiling, or maybe the best.

A study of Cognizant recognizes that profiling through IoT is one of the main trends in the future of IoT for business.

The change in this relationship can develop in the form of personalized advertising (Section 3.3). It will also be possible to perform an adjustment of prices and terms and condition following this pattern.

Car and health insurance companies, for example, are experimenting with personalised insurance conditions and 'Pay as you drive' or 'Usage based insurance' models.[12]

Companies also created ad hoc messages since they know who needs what. They are basically profiling in order to understand and respond to all different tastes. This can lead to unfair marketing practices.

The collection of these data exceeds in a strong concern about privacy, that we have already seen in the chapters before. Rules to prevent unfair commercial practices lead also the fair development of peoples' autonomy, privacy and dignity.

Analyzing the situation, it is a little bit like in smart cities, where citizens give information in order to have a better life. In this concern, consumers end up to give/provide data.

They are hence paying the service that they use with the providing of personal information.

[12] <http://www.heise.de/newsticker/meldung/Auch-Allianz-plant-Kfz-Tarife-mit-ueberwachtem-Fahrverhalten-2679007.html or http://uk.businessinsider.com/how-the-internet-of-things-is-transforming-the-insurance-industry-2015-7?r=US&IR=T> accessed on 15 November 2015.

Is for this reason that law started thinking about how to protect consumers. They end up with the conclusion that the important thing in order to let everything legal is the fact that consumers are aware of the fact that the data that they are giving are collected and then used (or better sold).

Under the EU authorities, Art. 5 and 6, it has been stated that consumers need to be informed in advance about the total price they are going to pay, also the non-material one.

Indeed, No. 20 of Annex tells us that also non-monetary forms of remuneration are forms of payments and should be considered.

The problem is with the fact that there is not comparison between data provided and dollars: it's not like a conversion between euro an pounds.

By the way, in the end, the important aspect of this situation is that consumers are informed about what is happening with their data, or at least they should not believe that they are having that specific service for free.

Another questionable point regards the following question: how far a company can go in collecting data in order to provide a service?

The main problem is to identify the consequences: although specifically tracked it is impossible to understand where data will end up.

Ethically speaking (Section 4.1 for more information) another important question is which extent is it possible to profile somebody in order to convince she or he to change their mind?

The main outcome that can produce this situation have been stated by Thal who theorized two cases: the situation of monopoly power with the consequence that the other party, typically the consumer, has no choice, and a situation in which the other party is weak.[13] Which actually is what we explained in section 2.3 regarding Facebook.

Before ending this parenthesis regarding IoT, is fundamental to understand that there is a difference between harassment, coercion and undue influence, although sometimes it's not really easy to underline.

Easier to go for examples, let's understand what harassment is: doorstep selling, phone calling and/or emailing possible consumers. It basically invades the private sphere of the person.

The thing that astonishes is that in marketing the only important aspect is how important is the need to find the right persuasion, in order to "capture" the hypothetical buyer.

[13] Spencer Nathan Thal, 'The inequality of bargaining power doctrine: the problem of defining contractual unfairness' (1988) 8 Oxford Journal of Legal Studies 17-33, 29.

In the end we can conclude that these new ways in which technologies are developing will or better, already have impacts on social life of people. We just have to understand how and in which direction law should act in order to prevent bad habits.

Indeed, in the next chapter, we are going to analyze in a better way how the topics develops in different countries in these years.

Implementation in Real life Cases

After an entire dissertation whose aim was to address and point out the different facets of an innovative and ever evolving concept like the one we are talking about, in this last chapter, it is of fundamental importance to describe in the specific what actions democratic nations, like United States, Germany and Italy, have implemented concerning the years that we are living in. In this regards we have already introduced some of these concepts in the paragraphs before (Section 2.4), above all regarding Germany and America. We did not analyzed our country with the right emphasis, but hopefully this is what we are going to do now.

We are going to analyze, for all the three different countries that we are taking into consideration, the history and development of the actions they faced while coming up with a such a complex subject.

5.1 United States of America

The United States is one of the leading countries in terms of development and innovations.

The US Constitution underwritten in 1789 was one of the most innovative and futuristic for the times in which it was written. It was for this reason that it represented an example to emulate for all other democratic countries. Although its innovativeness it was still deprive of an article concerning the right of privacy.

The United States of America had to wait until 1890 before the Right of Privacy was "published".

The Right of Privacy is an article, one of the most famous in the American legal history, published by Brandeis on the Harvard Law Review, which appointed the problem of new media regarding the invasion that they were undertaking on people's life.

Although the complains and the problems that still persisted there were not a body that took care of unfair commercial practices (which concerned also the subject of violating privacy). For this reason, in 1914 the FTC has been established. Since 70s this body has been the leading federal agency that is most often involved with privacy issues.

The theme became more and more important every day and it has been noticed also in the literature of the time: George Orwell wrote 1984 where it was described a city without privacy.

To implement the already quoted norms, the United Nations in 1948 published the Declaration of Human Rights in which, the Article 12, stands out exactly for its goal of protecting privacy.

Slowly the concept was started to be taken into consideration and more and more people become aware of the importance of the subject: it's for this reason that the layer Prosser, in 1960, published a new article where the four torts regarding privacy where stated.

He found out that there were the following problematic outcomes:

1. Intrusion in the public affairs of people;
2. Sharing of confidential information;
3. Ads that distort the image of a person;
4. Appropriation of people's name

In the years between 60's and 70's many legal cases regarded the hot topic we are talking about were discusses.

Eisenstadt v. Baird (1972) was a case regarding the possession of contraception by unmarried people. It was allowed following the right of privacy. Katz v. United States (1967) was a driving change cases: it extended the protection of the Fourth Amendment on the houses or any other place where the person has a privacy.

The 1974 states also another point in the scoreboard: FERPA Student privacy started to be taken into consideration. Basically there were the right of privacy also on the records of the students in any institutions.

In the same year it has also been published the Privacy Act which is one of the pillar of todays way of behavior in this field. It is a code of conduct.

Facebook, such as all kind of other social network is just the evolution of what enables people to stay in contact. In the years that we are talking about we saw the beginning of communication through devices. And what is the first tool used by humans in order to contact each other? Telephones.

Yes, exactly: telephones. We are not even talking about smart phones, but this is a topic regarding very old devices that are no more used nowadays.

In the chapter before we talked about telemarketing, and we can recall that it was one of the main way of marketing in the last decades of the last century. People got so annoyed from receiving unusual calls that in 1986 it has been implemented the TCPA and the National Do Not Call Registry.

These Acts regulated the telemarketing calls, prohibits same types of calls, and allow users to have the right of refusing calls like these.

Although the great strides that the country made in so few years, we see that only in 1996 the HIPAA (Health Insurance Portability and Accountability Act) has been enforced.

As the name states it helped the privacy of people in concern to their health and the information taken from hospitals.

Between the years of 1998 and 2000 it has been developed, both in US and in EU, the Safe Harbour Privacy Agreement which tries to avoid firms and companies to collect and share data regarding physical consumers.

In 2003 California was the first State that implemented a data breach notification law. It allowed agencies to know and share information on when personal information have been violated. Many other countries and states have shaped their laws taking into consideration this as a model.

Five years later the FCT and NUCA (National Credit Union Administration) in order to prevent identity theft, underwrote the Red Flags Rule.

California has always been a futuristic States for what concerns privacy rules. So it should be no surprise in uncovering that in 2020 it has implemented another Act in order to protect people data regarding how firms take advantage of these information.

It took the name of CCPA: California Consumer Privacy Act.

An year later also the state of Virginia's State enacted a Data protection Act and it will be followed by Colorado.

Probably many other States will follow this path, enacting in the short term regulations to protect consumers.

Actually the development that undertook in this history has had impacts on Facebook platforms and all other social networks.

In 2015 a problem was raised by a a guy placed in Ireland. He was really scared about the news that stated that NSA was using data collected from Facebook platform in order to control people. He claimed that the US privacy law did not ensure the adequate level of protection of personal data. He started to complain to the Commissioners located in Ireland. The commissioner rejected the complained as unfounded, because there was no evidence that his personal data had been accessed by the NSA. Moreover, because of the Safe Harbour Agreement, his complaint could have not been considered because the adequacy of data protection had already been discussed. The case was assessed by the High Court of Ireland and it stated that NSA was processing data for purposes that were overreaching the public interest. Moreover, it was stated that the Safe Habrour was invalid, because the processing of data for national security reasons must lay down clear rules to govern the application of the processing, to guarantee that the subject has the possibility to protect himself from the risk of abuse of data. Hence, since in the US the public authorities have the access to connect of electronic communications on a generalized basis, it was noted that in the USA there is not a high level of protection of personal data. Besides that, it has been emphasized that the National Privacy Authority might intervene in relation to all the personal data sent oversea.

What the NSA was doing with the Irish data revealed that all the principles were not respected.

Another agreement was concluded after this case, the Privacy Shield, in which the level of attention that us firms and institutions have to pay to our data is way higher than before: stricter obligations were imposed, together with heavier sanctions.

5.2 Germany

Thanks to this excursus we have had the opportunity to understand how the law in the US has developed in concern to privacy and data storage.

Now we are going to analyze how, the same topic, has been developed in countries such as Germany and Italy.

The three countries that we are highlighting have a deep democratic spirit, which basically means that they have the citizens and people safety at first place. This is the reason why we have decided to undertake a test on those, because if they are the places where safety and protection are at the center of their behaviors, and maybe they are not doing the most to guard their interests, can we imagine what other countries, where their safety is not considered, can do?

In this dissertation we are not able to give an answer to the difficult question of if they are doing the most they can do, but we are going to leave this result to all those who are going to read it. This last chapter is not the only one to take into consideration while elaborating response, but we advise the reader to take into considerations all the cases mentioned in this paper.

In order to start talking about the last two countries that we have to analyze, we can start to underline some guides that both Germany and Italy have in common.

In the history timeline, since both countries are part of the Eu, we can highlight a little excursus on the European law regarding privacy and data protection.

We can say that everything started in 1995 with the EU Data protection Directive, where the concept of privacy had been way more developed compared to the USA.

A step that can be considered of fundamental importance is the fact that in the 2012 has been implemented a right that enable people to decide if they want to be withdrawn by an IT system. It takes the name of Right to be forgotten and had received a great appreciation from many people.

Although the effort that the European Union is doing in order to protect and ward its citizen, they did not actually stop there.

Indeed in 2018 it has been developed and implemented the GDPR: the General Data Protection Regulation.

It was a way of change and innovation since the regulation established in it are applicable also to the transfer of data outside of the UE and EEA.

Now we are going to go a little bit further in the analysis of German data Protection.

Germany places a great deal of impotence on privacy and data protection. They indeed prohibit any kind of data storage (of course with some exception but still…). It also can change in case the person gives its explicit consent in the storage of its information.

Actually, it must be highlight that data protection is not explicitly written down in the Germany's constitution but anyway it is established by the virtue of the 'census ruling' by Germany highest court.

In 1983 it has been decided that every kind of individual had the right to decide concerning its own data.

Although not many people think about it but also the World War II had an impact on how German people deal with protection on data. These years, that represent an abuse of privacy for the citizens had left people with the strong desire of having control on what concern themselves.

The FCC (Federal Constitutional Court) published many Acts concerning this sch as the Telecommunication Act and the Federal Data Protection Act.

This is really different from what happens in the US, where they have different Acts for different kind of privacies. Here instead there is just one Act (Federal Data Protection Act) that safeguard everything.

The law has been revised and changed during the years, but it still influenced by six main pillars:

- Ban subject to permission
- Data economy
- Transparency
- Direct collection
- Necessity
- Purpose limitation

In order to understand a little bit better the mentality that governs these decisions we have to understand that in this country privacy is strongly linked to consumer welfare.

Indeed, they decided that the way in which Facebook was behaving was a harm for the citizens.

In Germany privacy has been considered in terms of consumer welfare: different kinds of privacy protection. Facebook was accused of violating consumers privacy because it does not provide its consumers the possibility to choose the level of privacy protection.

There are still, anyway, problems concerning how much firms can interfere in the acquisition of data. Some politicians in Germany believe that it is of fundamental importance allowing companies to improve services offered.

From an international point of view (foreign policy) since Angela Merkel was the head of the country, Germany always waited the development of the situations. In concern, for example, of the Snowden case, she only expressed herself and condemned the action when she discovers that also her phone was under surveillance.

The position of Germany is quite clear anyway. It is impossible to argue in a different way: it is one of the countries which takes in large consideration the privacy of its citizens and is undoubtable that they are not doing the most in order to prevent dominant positions of firms that can flow in privacy problems.

Now that we have analyzed two different points of view, we are going to highlight all the characteristics of an innovative country such Italy is.

5.3 Italy

For what concerns Italy the first regulation that implements data protection was the law n. 675/96. Afterwards it has been drawn up the Legislative Decree of 2003. In Italy, such as in Germany, the Constitution does not have any reference of privacy but thanks to Article 14 (inviolability of domicile) and Article 15 (confidentiality of correspondence) it has been recognized as a fundamental right.

For this country GDPR plays a crucial role since Codice in materia di protezione dei dati personali, has been drawn up to it.

Anyway the most important law regarding these is represented by Legislative Decree 101/18.

Thanks to this, Italy has elaborated on many aspects that otherwise would have not had been developed.

The first one regards the age of consent: a child over the age of 14 can consent on the process of his/her data. From this we can understand why Facebook is forbitten to them.

The Code express itself also in concern of employment relationship. For example it has been forbitten an investigation or process of data of workers on the basis of personal beliefs.

It has also been forbitten the use and hence recording of workers.

In accordance with Article 105 of the Code, personal data processed for statistical or scientific research purposes may not be used to take decisions or measures relating to the data subject, nor for other purposes.

For what concerns Facebook and its development in the country we can appoint a specific episode that happened in 2019. It is the case regarding Cambridge Analytica, where Facebook has been fined 1 million euro by the Italian Dpa (Garante per la protezione dei dati personali). Its behavior has let authorities bewildered regarding how a company can actually exploit information. It represents the first and biggest exchange of data that the world has ever seen.

Although what the word face, Italy, we can say, remains always a country where the issue remains at the margins. Few are aware of the real problematic that it is faced and Italian law is now moving the first steps in this direction.

We can just wait until more and more lawyers, but also citizens, will take more care about their privacy and sharing of data with platforms that actually strumetalize them.

In the end we can say that it has been of fundamental importance the development of Facebook and it has started, at the beginning of the century, to creep inside the life of everybody.

History and 'personal' experiences of each country have instead played the rest of the game.

Regulations differ from country to country, but they still follow the same guideline. The interventions of Courts (such as FCT or CJEU) may have or will provide important guidance.

In the meanwhile it's still difficult the monitoring of navigation of individual, even just surfing in the internet could be difficult. Not, of course, from a systematic point of view but from a reglementary one.

Thanks to this cut of now we are able to identify and understand what and when applications have been enacted to monitor the exploit of this kind of communication tool better know as Social Network.

Conclusions

Data spread by users and collected by firms play nowadays a fundamental role in the society we live in.

Globalization, the economic cries and the diffusion of new IT channels, all mixed together have changed the competitive field where companies play.

Corporation but as well costumers had to face new challenges, that never before came up in such a context.

All through this dissertation we have highlighted the evolution and the way of how data collection has been able to become such an important tool.

In these concern we have seen that the only subject that really can help regards law and all its implementations.

After this analysis we can point out a valuable line of conduct that in some way has been the same and sometimes inserted could not be more different. Countries differ on the decision they took regarding how to safeguard data of users and at the same time tempt firms to capture and elaborate as much information as they can. In the end data analysis could be useful also for them.

We have not gone through the explanation, or to better say investigation of countries and nations that can not be classified as democratic. In these countries by the way, governments perform themselves profiling and usually, in order to give better services to their citizens exploit and take advantages of these actions.

We have seen that in the democratic nations we have taken into consideration, likely it is not the case.

Although America is a little bit freer, now they are trying to implement new rules and they start having interest in take care of their citizens.

Germany on the other hand is way more ‘armored’ we can say. In the sense that they really fear data exploitation and for this reason are trying to implement as much laws as they can.

Italy instead is now taking in real consideration the topic. Although the high influence that European union and their actions had on this country, we are a little bit far from other countries. We have many rules but it is in these years that we started elaborating on them.

In conclusion we can say that the topic is still now an ever-evolving field, and it is quite hard to fix a point and explain carefully and in depth it.

Italy is now doing the right work and other countries are following the same path.

We can only hope that in the future this topic will be taken in consideration with the real weight that it has, and that both parties interests will be protected.

Bibliography

1. *Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. SSRN Electronic Journal . doi:10.2139/ssrn.2477899.*
2. *Ward, Jonathan Stuart, and Adam Barker. "Undefined by data: a survey of big data definitions." arXiv preprint arXiv:1309.5821(2013).*
3. *Database Systems Journal vol. III, no. 4/2012.*
4. *American Journal of Software Engineering and Applications.*
5. *Richards, Neil M. and King, Jonathan, Big Data Ethics (May 19, 2014). Wake Forest Law Review, 2014.*
6. *A. Giannacari. Facebook, tra privacy e antitrust: una storia (non solamente) americana (2019).*
7. *M. Winerman. The origins of the ftc: concentration, cooperation, control, and competition.*
8. *Laura Phillips Sawyer. US Antitrust Law and Policy in Historical Perspective (2019).*
9. *Arnold Roosendaal. Facebook tracks and traces everyone: Like this! (2010).*
10. *Dr. Christophe Carugati. The Antitrust Privacy Dilemma (2021).*
11. *Clarke cooper. Facebook question,*
12. *Christian Fuchs. Propaganda 2.0: Herman and Chomsky's Propaganda Model in the Age of the Internet, Big Data and Social Media (2021).*
13. *Sanna venere stefania. Controllo, sorveglianza e resistenza attraverso il social web. Alcune esperienze italiane a confronto (2014).*
14. *Thorsten quandt lena frischlich svenja boberg and tim schatto-eckrodt. Fake News (2019)*
15. *Facebook e il monopolio della censura. Problemi dell'informazione (ISSN 0390-5195) Fascicolo 3, dicembre 2018.*
16. *O. Ambroso, A. Beulcke. Click Propaganda (2019).*
17. *Cristopher Cepernich. Le campagne elettorali al tempo della networked politics (2017).*
18. *Prof. Dr. Natali Helberger. Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law.*
19. *Alvar C.H. Freude and Trixy Freude. Echoes of History: Understanding German data Protection.*