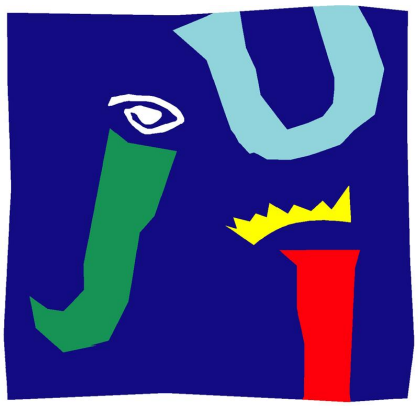
Facebook: The Business of Web Ads and Data Processing



UNIVERSITAT JAUME·I

Bachelor's Degree in Economics Course 2022-2023

Tutor: Nikolaos Georgantzis

Manuel Domingo Gómez al385337@uji.es

1. Abstract:

This paper focuses on user information on the internet, specifically that which is available to Meta along with a review of how it is obtained and classified for marketing. Privacy policies and cookies for purposes other than those of the consumer along with the scandals and controversies surrounding this.

A review of the historical context to get to the great power available to the company, the regulations that accompany this process and its hardening in the wake of events in which Meta has been involved.

Highlighting the voluminous data leak by Cambridge Analytica through its association with Facebook for subsequent use for political purposes among others. And the consequences of this.

Followed by a review of the European framework and the direction it decides to take in the near future with regard to the rapid advances in technology and the need to protect people in their browsing on the web.

Finally, a reflection on the reality we live in, the misinformation, numerous empty stimuli accompanied by unnecessary consumerism and how unprotected we really are. In order to give our time and security the importance it deserves.

Keywords: Facebook, misinformation, internet, privacy and security

Facebook: The Business of Web Ads and Data Processing

Index:

2. Introduction:

The motivation of this work is to expose the situation experienced in terms of the possession of information and monopoly practices with the available resources.
This condition related to this economic action is analysed and reasoned throughout the document, developing conclusions and actions that favour and make this situation possible.

The measures and sanctions adopted by governments to ensure sustainable development are reviewed objectively. It begins with the birth and history of the company that managed to store data on a massive number of users, and concludes with everything it unleashed.

Facebook is a company founded in 2004 by five Harvard University students (Mark Zuckerberg, Andrew McCollum, Eduardo Saverin, Dustin Moskovitz and Chris Hughes), initially aimed entirely at the university's own student community to facilitate connections between them. But due to its success within the university, it spread to most universities in the United States, even reaching Canada at the end of 2004, when the total number of users was close to one million.

This was followed by his association with the founder of Napster, which allowed him to be known in a different field and the arrival of the first rounds of investment.
Later in 2005, 'The Facebook' was renamed Facebook, closing the year with around 6 million monthly active users and the implementation of the tagging of people in photos. The following year (2006) was the one that consecrated the platform for the global opening, innovation in design and the incorporation of the newsfeed that has been so key.

Along with new functionalities that were added, such as Facebook Marketplace or Facebook Application Developer, for the development of apps and games within the platform by developers, among others. The variety offered by the platform in 2008 made it the most visited social network, surpassing MySpace.
Also noteworthy was the birth of the 'Like' button in 2009 and its milestone of being the most popular social network in the world that same year with 350 million registered users and 132 million unique monthly users.In the following year, Facebook was valued at more than 37 billion euros, making it the third largest web company in the US, behind only Google and Amazon.

Looking back to the present day, at the Facebook Connect in October 2021, the change of name was announced as a result of the orientation towards the metaverse.

Meta is how it was renamed, and is also where platforms such as Instagram belong, acquired in 2011 to coincide with Facebook's IPO year and the achievement of 1 billion monthly active users.
Or Whatsapp, acquired in 2014, after failing to acquire Snapchat, where it opted to copy the platform's appeal and add it to the platforms under its control.
Other curious companies are Oculus VR (a company focused on virtual reality) and Gipghy (a leader in visual creation and expression) which are part of this group.
Finally, Facebook prioritises expression, but does not deny that the Internet creates opportunities for abuse that in some ways expose its consumers.

Facebook reasonably has a set of community standards or guidelines to help protect its principles.
But sometimes journalistic and public interest prevails in such situations so that content is censored, based on the protection of one of four core values: authenticity, privacy, safety or dignity.
The most important value we are going to focus on is privacy, both in terms of the way in which it is approached and the way in which it is dealt with.

Understanding that the main tools used by Facebook are Artificial Intelligence tools with the mission of identifying and eliminating content that infringes the community's rules.

We reasoned that a human role is necessary in specific cases to verify whether the guidelines are being followed, so they are referred to these personnel with the aim of reviewing and issuing a verdict on whether the word or article being dealt with is appropriate by evaluating its context and making sense of the wording used.

If it is confirmed that the content violates Facebook's community standards, Facebook's 3-step enforcement protocol is applied: remove, reduce and report. Removing the harmful content so as not to contribute to the disinformation that is so prevalent today, reducing its appearance on the platform through recommendations or simple

appearance in the feed and finally informing the sender of inappropriate behaviour along with warnings in the content itself so as not to misinform any consumer of the issue at hand.

3. Advertising (Facebook Ads)

After reviewing Meta's history and how it has evolved over time, it is important to talk about one of its biggest businesses: Advertisements.
Among the services offered by Meta to help businesses, there is no doubt that Advertising or Facebook Ads, commonly known as Facebook Ads, aim to promote products and services through publications or text, image or video ads.

This platform of sponsored ads, which appear in the news section for all users who use Meta group services, where the appearance in the feed is managed after an agreement between the advertiser and the platform, providing a crucial utility for the online marketing of many companies.
Its differential feature is due to the segmentation between different groups of users that the platform offers, from personalised audience, age ranges, gender, location and language.

Together with the integration in the feed giving it the same visibility as a user publication which the user has voluntarily followed, a recommendation of content without commercial purpose or recommendations based on the connections within this social network, viralization as an attribute pursued since the interaction allowed and the analysis of the results of the campaign launched through tools provided by the web interface itself. There is nothing better than knowing the tastes of a consumer to be able to sell them something they need or believe they need to benefit both parties, but at what cost.

The cost comes with the problems of the service, the numerous controversies that have surrounded it in recent years are impossible to hide due to violations of the privacy policy, its lack of transparency and association with actors of dubious honesty, the precision and resources it offers give Facebook and Meta in general a great power of information about users that, if not treated properly, ends up being exploited without any kind of limit. With great power comes great responsibility, in this case the power of information.

3. 1 Ad Category Analysis

To reinforce these scandals, we will use as support a study of 600 real users who, through an extension in their browser (AdAnalyst), record the ads they receive and the limited explanation of why they receive them.

We studied 89K/146K ads and 22K/28K advertisers, the importance of this study lies in the wide range of ads available on Facebook compared to other social networks by the companies that make up the Meta group and the broad spectrum to be covered.

We must question the use that the platforms make of the data because their transparency is so dubious that to the surprise of the public they do not report the real use, so that information that we would never want to share may be compromised.

One issue that should be a cause for observation and concern is how easy it is to be an advertiser in this environment, as the steps to be taken are simple and with precise explanations to speed up the process and increase business, thinking more about figures and monetising users than about the users themselves.

So we can even enter into levels or ranges where advertisers group their target audience according to a series of criteria or keywords in their searches. This starts to be a little intrusive but becomes more so and accentuates its intrusion when we talk about Personally Identifiable Information (PII) on personalised audiences, where they have full knowledge of the users to whom the product is directed.

Expanding on this Personally Identifiable Information, it is clear that this private personal data should not be in the hands of a large company with zero social responsibility.

Even on the basis of the personalised target audience, there is the possibility of asking Facebook for audiences with similar characteristics by identifying themselves and adding to the selection something so routine that it seems to lose the danger of playing with the information of groups of people in this way.

By consulting Facebook's timeline and the limited explanations offered by the browser extension on the reception of advertisements, one tries to reach a conclusion,

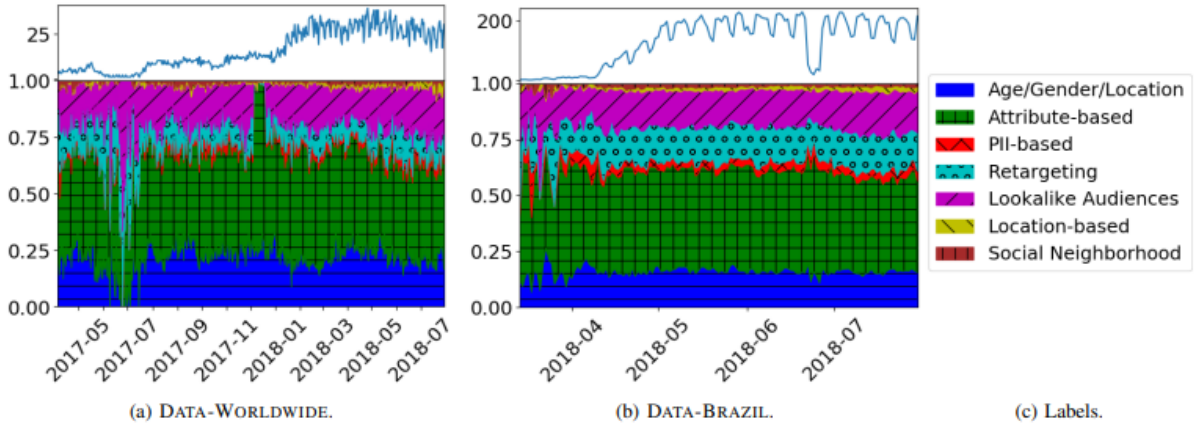
especially on issues such as election campaigns, due to the importance they have on the population and the obligation of transparency.

At least one measure that works in Facebook's favour is the need to have a page on its portal which offers information about the advertiser, something that was not previously defined in this way and which increased the uncertainty about who defined the content even more.

The purpose of consulting the data obtained through the study carried out on advertisements in a global framework and also focused on a region, in this case Brazil, due to the proximity of elections and to see how these can be conditioned by the advertising received by voters, is to be able to explain audience selection patterns or segmentation methods.

In order to clarify the organisation of the advertisements, we will use the following image to comment on how they are distributed:

Figure 1: Targeting Criteria across time. Above: daily number of active users



Source: A. Andreou, M. Silva, F. Benevenuto, O. Goga, P. Loiseau, A. Mislove, 2018

It represents the evolution of ad targeting measured over a period of time, from May 2017 to July 2018, with a daily tracking of the fragmentation of the advertisers' side of the advertisers with respect to the total number of ads collected each day through the browser extension.
Being able to analyse the type of combined data used and explain the why and how of this selection.

3.2 Audience Selection Criteria for Advertisements

First of all, in order to understand it better, we will talk about age/gender/location as basic or more generic criteria; when it comes to specifying them further, we will go into the characteristics selected by the companies, which will be taken into account by data held by Facebook, provided by third parties or obtained by themselves through various methodologies.

To talk about the diversity that is born in this selection, we go into the redirection of the campaigns, dedicated to a target audience whose interaction has existed at some point in the past so that the users themselves motivate the reception of advertising by the company concerned.

It is also possible to fall back on something more commonplace, such as location, provided by users but implemented with location awareness permissions as a measure, to choose the audience to receive the advertisements, in addition to lookalike audiences, chosen by similarities with previous selections or results that are detected by competent artificial intelligence and inundated with this type of marketing.
The term "social neighbourhood" refers to the friends of users who have provided feedback to a company through social networks. Due to their shared tastes and generalisation of consumption patterns and movement in specific environments that arouse common interests, this advertising is applied to them.

Now, after defining some processes, it is time to enter into the percentages represented in the image in order to draw conclusions.

Age, gender, and location, which is regarded as the most fundamental targeting criterion, accounts for 19% of ads, while ads based on specific traits account for 47%, and ads based on interests account for 39%. We can infer from their evolution and disposition that they prefer prototype profiles to covering a greater mass of the population without such specificity; they are more interested in anything concrete as a strategy to reduce the circle of options than simply focusing on the generic set.
According to a new social media ad targeting approach that enables advertisers to request Facebook ad distribution based on prior ad campaigns, as previously said, 17% of ads target comparable groups.

The problem with this targeting mechanism is the algorithm on which public audiences are based, which creates absolute uncertainty for users due to the impossibility of knowing why they have received it.

12% of the ads are part of retargeting which means that an advertiser is trying to reach a user, previously already in contact with them, while a small part of the ads, 3%, are part of PII-based targeting.

A large number of users, 79%, have been targeted by at least one ad based on PII targeting, meaning that the advertiser knows the user's email address, phone number or other information such as home address. This is quite alarming and highlights the companies' monopoly of information about the user.

There is no perfect verification process to find out how this information was obtained, but it is true that it can easily be bought online or obtained through the leakage of personal data caused by security vulnerabilities.

Such events are very common, a major scandal in 2019 was the leak of more than 770 million email addresses and 21 million passwords on MEGA, a cloud service that was branded as a major hacker forum. Events like this do not look for patterns of behaviour as opposed to treated companies but for maximum exposure.

Segmentation by social neighbourhood accounts for only 2%, which is unexpected, given the competitive advantage this strategy gives over traditional media.

Table 1: Targeting of advertisements by region

	Europe (85 users)			North America (16 users)			Brazil (495 users)			Rest of World (12 users)		
	Ads	Advs.	Users	Ads	Advs.	Users	Ads	Advs.	Users	Ads	Advs.	Users
Age/Gender/Location	24%	35%	98%	19%	25%	94%	16%	28%	94%	18%	28%	75%
Behaviors	1%	2%	39%	1%	1%	31%	0%	0%	0%	1%	2%	50%
Demographics	2%	3%	27%	1%	2%	31%	0%	0%	0%	1%	3%	33%
Interests	37%	48%	94%	23%	36%	88%	41%	55%	97%	41%	48%	92%
Profile data	7%	8%	88%	4%	6%	88%	4%	5%	83%	9%	11%	75%
Data brokers	1%	1%	28%	2%	4%	50%	1%	2%	49%	0%	0%	0%
PII-based	2%	1%	73%	6%	5%	81%	3%	2%	80%	2%	2%	67%
Retargeting	8%	7%	80%	13%	13%	94%	15%	12%	95%	10%	10%	92%
Lookalike audiences	17%	17%	92%	30%	33%	100%	17%	14%	96%	15%	19%	83%
Location-based	1%	3%	71%	2%	3%	50%	2%	6%	63%	1%	2%	50%
Social neighborhood	1%	3%	51%	1%	2%	62%	2%	8%	61%	1%	4%	58%

Source: A. Andreou, M. Silva, F. Benevenuto, O. Goga, P. Loiseau, A. Mislove 2018

Finally, to contrast segmentation globally, we will analyse the data obtained for each type and the geographic regions they represent.

Data brokers and PII-based targeting are more prevalent in North America (by 1% and 4%, respectively) than in Europe. Surprisingly, 81% of users in North America have encountered this kind of advertising, which is 8% more than in Europe (73%). Due to these societies' reluctance to share their data in one location and in another, coupled with the values and education they hold, it is interesting to consider the relationship this may have with privacy laws and the handling of personal data, as well as the culture that surrounds these societies.

Linked to this reflection is the fact that European advertisers focus more on Age, Gender and Location; so in some ways it is more 'respectful' than marketing strategies used in other parts of the world, with privacy having a greater weight in this region.

In the Brazilian region, advertisers spend most of their resources on interest-based advertising, which is in line with Europe and the Rest of the World, but different from North America, which prefers to opt for Lookalike Audiences.
Specifically, in the Brazilian region, 41% of ads are based on user interests, with 55% of advertisers allocating resources focused on this category and reaching 97% of users, figures very similar to the rest of the world, although in this region they are slightly lower.

In relation to what was discussed above and with the aim of better intertwining with the topic below, it is interesting to comment on the before and after of the GDPR (General Data Protection Regulation) policy introduced in Europe in 2018.

Its link to PII is obvious so it cannot be overlooked, going back to the fact that 73% of European users have been reached through PII based segmentation and data brokers we arrive at that represents 40% of the European population, something undoubtedly astonishing.

So let's try to see how effective the measures introduced in that year were and how they evolved. One of the first surprising facts is how cheap it is to disclose a person's privacy online, this study estimates that the cost of disclosing a user's identity can range from €0.015 to €1.5 depending on whether the success rate in obtaining information is higher or lower, a really ridiculous figure for something so valuable.

The population in question, Europeans, have fairly refined criteria so that levels of trust and their willingness to give information in exchange for services are limited, something that in other parts of the world may not be seen to be the case and therefore more likely.

An important step in this policy is the prohibition of sensitive personal information such as unspecified but assumed or taken for granted sexual tastes, unless there is explicit consent, in which case there will be advertisements of this type.

As an interesting fact in Spain a case like this, of personal information, without explicit consent brought a cumulative fine of 1.2 M to Facebook for violating the Spanish data protection law since 2015 with two fines of 300,000 euros and a more serious one of 600,000 euros, the resolution of this case in 2017 was mediated by the Spanish Data Protection Agency (AEPD).

It is interesting to note that women are significantly more exposed to ads than men and that the most vulnerable age group is between 20 and 39 years old, above all other groups.

Within the Facebook Ads Manager, the most important parameter related to this information is the potential reach which identifies the number of registered Facebook users that match the selected audience attributes.

Also noteworthy is the role of 'The Data Valuation Tool for Facebook Users' as a valuable resource for these users, as it provides a real-time estimate of the revenue they generate for the platform based on their profile and the number of ads they view and click on during their session.

The conclusion reached is that the explanations about the reason for each ad are incomplete, because they only highlight one of the many attributes they can use to define their target audience, so here we would enter into the conflict of the tremendous inequality of the information that Facebook possesses and cedes to other companies compared to what the consumer has and can obtain.

Even though it has been ceded by the latter without knowing its true usefulness, we enter into the justification of why this practice ended up in lawsuits and the numerous scandals involving the company. Fortunately, a lot of work has been done and continues to be done to balance the balance of information and to reach the consumer.

After having talked about the functioning of the advertisements, let's try to draw conclusions and learn a little about the dynamics that are followed depending on the part of the world. Let's talk about a case that left no one unmoved by its social impact and the importance of the leaks in so many areas. Let's start with a review of the creation of this company and everything that surrounded it during this period.

4. Cambridge Analytica case

Firstly, Cambridge Analytica, founded in 2013, is a data company, more closely related to the political sphere. It has come to be categorised as a clandestine political consultancy, and formed a close link with Facebook due to the information flows between the two.

Known globally for the great media uproar, after it became known that it came into possession of sensitive personal information of more than 87 million users, something that was facilitated by Facebook and that jeopardise the security, privacy and well-being of any person related to the platform.

From its beginnings in obtaining data until 2018, when this great event broke out, it had gone relatively unnoticed until the curtain was lifted and everything that was behind it was really seen, we frame this stage as a manipulation of information with absolute freedom, after which governments and institutions helped by researchers and technologists set about developing privacy policies to cover cases like this.

In parallel, it is necessary to comment on the creation of Global Science Research as it ended up complementing Cambridge Analytica, following a clear methodology: new technology but old strategy.

Aleksandr Kogan together with other colleagues related to the University of Cambridge created this company with the aim of marketing a Facebook application called 'this is your digital life', which collected personal information from participants which, unlike the initial purpose of Cambridge Analytica, in this case the main objective was to obtain potential information in the political sphere, although it was oriented towards users in the form of personality tests, and this is how they managed to obtain it from more or less 50 million people.

Their procedure began with Facebook personality tests of volunteers by researchers connected to the University of Cambridge.
To assess their psychological profile, 'OCEAN' (openness, conscientiousness, extraversion, agreeableness and neuroticism) assessed these attributes by linking them to Facebook profile activity for a more complete analysis.

The major finding of this study was how useful the procedure was for psychological profiling without resorting to a formal psychographic instrument.

In this first experiment, there is no evidence of abuse of participants' privacy or sharing of results and criteria.

After this, it was renamed Cambridge analytica, and its next step was to collaborate with Global Science Research, where the partner company in question, GSR, requested access to participants' personal profiles, which allowed full access even to their links on the platform; keeping this data was not at all necessary for the research, as the main mission was to develop a methodology for psychological profiling, not to complete databases.

But predictably, they did store it, because of the potential of knowing this data and the possible integration of information in a broad-spectrum and scalable business.
Examples of its use can be electoral campaigns such as Trump's, which we will talk about later, by creating messages or simply internet content that sought to influence who it was aimed at, so that those who were clear about their decision would be motivated to make it, and those who doubted would be completely put out of their minds.

It is worth mentioning the access to information, even though it is not part of Facebook, its ecosystem and resources are so extensive that, for example, by means of cookies on web pages, they can extract what they want. An almost intuitive action where most of the time we do not know what we are accepting.

The selling of this information is what happens in this process of extraction and ultimately playing without rules by combining truths and lies with the sole aim of influencing the user.

The story was made public by Christopher Wylie by way of making it clear how far the handling of our information had gone, ensuring Facebook's full knowledge of the data processing since 2015.

Until this data has real-world use it is not given the importance or added weight it deserves, evidencing its influence in the 2016 Trump election, not only on levels of utility, but also in a way critical to tipping the balance.

Accusing it of collusion with Aggregate IQ surrounded by controversy for also being involved in some Brexit referendums are ways of assessing its large societal impact. Decisions of society are influenced by precise stimuli on the web.

Followed by multiple denials by the sides involved to avoid any legal consequences.
Something that also had Trump in its sights as Robert Mueller tried to expose him for election tampering but was constrained by US law which prevented him from charging a sitting president.
If we provide historical context on voting in US history, we see that the distortion of electoral preferences has always accompanied it, making sense of Elbridge Gerry and the derogatory term 'gerrymandering' associated with the manipulation of these elections back in the day.

The confusion of the adversary also expands this culture, used by John F. Kennedy exploited the environment to his advantage, other cases include the production of false documents in order to discredit, wiretapping that led to convictions and imprisonment of Republican party CEOs, and a long history of events that reaffirm an ever-present manipulation and extortion.

In addition to elaborate techniques such as the selective allocation of polling places, voting times by constituency, use of purge lists or reduction of voting opportunities by mail-in ballots or early registration by reading these kinds of deceptions are quite shocking as they seem to be from another era but the only thing that differentiates them from the technique employed.

Cambridge Analytica relied on technology This reaffirms that no matter how much evolution and progress we continue to fall into the same banalities, power ends up corrupting, trying to take everything behind it even if its arguments and programmes do not have a solid base on which to build.

The birth of 'micro-targeting' was another danger elaborated in this process, through highly influential individual messages to targeted users in order to modify their behaviour, empowering the holders of large user databases in a very dangerous way.
It results in microtargeting of niches that are easy to corrupt if one knows which points to touch, something that the information makes possible.

The core of this information lies in the science behind it, and we will delve into it thanks to Cathy O'Neil's 'Weapons of Math Destruction'.
The author, as a data analyst, explains the dangers of not using data patterns in an objective way, as the data itself is not the danger but the use of these, the problem is the poisonous overlays camouflaged by mathematics that are not tested or questioned, because if the process is configured to react through certain elements that it looks for in that information, the problem is the configuration.

An example might be a mortgage algorithm determined by traits such as ethnicity or gender, a computer has no knowledge of these and the real concern is that it is programmed to react to them.

The over-reliance on these is referred to in the play as the dark side of data because of the dire consequences it has brought with it, both the crisis of 2008, and a worse way of grading university education because of the poor evaluation and reconsideration of the data obtained.

The reflection on this is the bittersweet sensation that it leaves with it, because although manipulation has been a more than evident practice in this electoral process, it is also true that the problem stems from being influenced by stimuli received on social networks or the internet as a whole.

Without independently verifying the veracity of these supposed arguments, we have lost the context and as a consequence we are only interested in sensationalist data, rather than contrasted information on which to base our opinion, therefore the problem originates in the criteria of each person and this perversion of opinion.

Also leaving a message of professionalism in performance, a UK Channel 4 investigation claimed that Cambridge Analytica, acknowledging that it ran the Electoral College for Trump in 2016, only influenced 40,000 voters in three states.

Something that would have helped him to get away with it if it had not been for the statements extolling his role by executives of the aforementioned company.

Finally, it is worth noting that there were several forces manipulating the elections, only this company would not have had such an impact.

4.1 The effects of malpractice

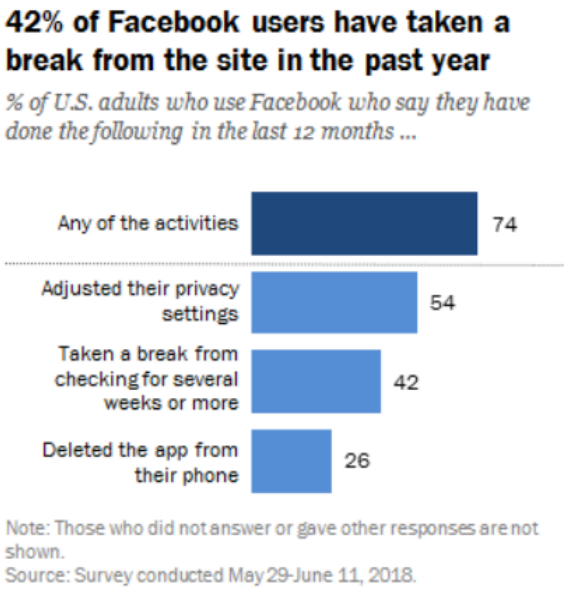
As in any business, it is reasonable to think about the consequences for the product offered, in this case a service, when so much information about it comes to light. To the point of distorting the brand image and the service itself.
Is Facebook a social network and advertising portal with the aim of bringing people together?

Or simply an information business that has never really declared its intentions?
We will try to shed some light and draw some conclusions about a long-standing shadow operation by looking at the variations in its use over time, the legislation imposed in different parts of the world and, above all, the future planning of such measures.

4.2 How has this affected the use of Facebook in recent years?

As evidence of this poor performance, let's look at how US users changed their consumption habits after hearing the news via an study carried out in 2018 highlights the relationship of users with this platform in the wake of the Cambridge Analytica scandal among other reasons surrounding so much controversy

Chart 1: Change in facebook usage over the last year, at 2018



Via: Pew Research Center

To clarify the above, we will focus on three actions carried out by users in the last year, as the information obtained shows that 54% of the users surveyed have modified their privacy settings, which undoubtedly shows the user's distrust and insecurity due to so much news on this subject.

Evidently it is logical to think that if something compromises the user, they should modify their behaviour, and what better way to modify their habits than by taking a break from Facebook for several weeks, something that represents 42% of the US population. But not forgetting what a more drastic type of user would do in this case, uninstalling the application, with 26% of the total participating in this case.

Seventy-four per cent of users have carried out some of the actions described above, showing that no matter how much business is done at the macro level by large companies through advertisements or the sale of information, without the users who make it possible, it is unsustainable.

Even when they do business behind their backs, treating the situation as alien to the actions of the company itself, without respect for the consumer, the business will hardly prosper and will even cause absolute disillusionment on the part of its final public, which will be affected at all levels.

When analysing the type of public that is most likely to take initiatives in the face of enlightening information, users in the 18-29 age range are those with the highest percentage, 44% specifically, of total users in this age group who have uninstalled the application compared to 12% of users over the age of 65.

This quantitative data sheds light on the growing concern about information nowadays, and giving the weight it has to something so valuable. Nor is it possible to be completely objective, since it is logical to think that older people are less concerned about the Internet, compared to people of working age in a labour market of continuous adaptation, and where keeping informed is an obligation rather than a whim.

It is true that the percentage of data adjustment increases to 33% for people over 65 years of age and 64% for younger users.

In relation to the case that everything revolves around, of the users who downloaded the information collected by Facebook that was available about them (approximately

9%), this percentage of users did take action and 47% uninstalled the application from their phone along with 79% who opted to modify their privacy settings.

These figures are very relevant and are food for thought for the company.
The greater the awareness and importance of the events that occurred in 2018, the greater the rejection of personal information being breached. According to a world with so many stimuli, scams and needs, age groups with a peak of activity either for work or concerns take action for injustices and try to change the reality in which they live.

The migration from the web2 in which we currently operate to the web3 as a means of decentralisation with respect to information giants and thought controllers may be imminent.

Everything will depend on the desire, initiative and interests of those who develop it, as there is no greater obstacle than powerful companies that do not find it profitable.

Facebook obviously wants to be part of the change, but organically it is a big debate, its change of name to Meta is a declaration of intent along with initiatives such as virtual reality. For the moment these are just projects to be developed and to which a lot of effort will be devoted, but after all that has been experienced, it is obligatory to pay attention to the treatment of the user when entering the infrastructure that we are about to glimpse. Advances in technology seem to be in their infancy, but total control is too great a risk to run without demanding certain principles and criteria.

5. European Agenda 2030

5.1 SWAMI Project

As we mentioned before, it is necessary to develop through principles and criteria, therefore these are the ones that the European Union intends to follow in the near future. We review the 2030 agenda to see which points they have decided to focus on and how they are going to do it.
For some time now there has been a great deal of interest in privacy policy, an example of which is the SWAMI project funded by the European Commission in its Sixth Framework Programme.

The project started in February 2005 and lasted 18 months and consisted of five partners: the Fraunhofer Institute for Systems and Innovation Research (Germany), the Technical Research Centre of Finland (VTT Electronics), the Vrije Universiteit Brussel (Belgium), the Institute for Prospective Technological Studies (IPTS, Spain) of the EC Joint Research Centre, and Trilateral Research & Consulting (UK). Risk assessment in different possible scenarios due to the power that artificial intelligences were gaining and the large amount of data they possessed through continuous data mining.
An example of action could be to identify the 100 most critical technologies in the next 15 years, or the most important factors influencing the development of a certain technology and/or the most important actors.

The methodology consisted of a structure able to analyse by constructing and deconstructing scenarios.

The problems identified were hackers and attackers, proliferation of functions, surveillance, profiling, lack of public awareness or concern for rights, lack of enforcement and oversight, erosion of rights and values, uncertainty about what to protect and its costs, government and industry not being transparent about what personal data they collect and/or how they use that data.

The focus on legal, technological and socio-economic domains calls for privacy audits and some form of cooperation between who provides information and who uses it.
Increasingly secure anonymity with the taking of precautions and alternatives of movement on the web. As a result, serious legal problems were identified in applying measures in such a dangerous and changing environment, with transparency and protection being the best ways to counteract any future problems. Obligations on the authority or employer to collect information and a private sphere of the user where the invasion of that privacy requires explicit consent.

The goal towards which the European Union is moving is a democratisation of knowledge about technology both in basic skills and in greater specialisation about ICTs.

In companies, a greater technological implementation, trying to reach 75% of companies with the use of contemporary advances, whether big data or Artificial Intelligence, due to their use in daily activities and the severe delay that this would entail both to the need to have them available for market assessment. Not taking a step

in time is to be left behind; technology at this level is more than the future, it is the present.

Another somewhat shocking measure is the identification of at least 80% of the population in digital form, physical format in case of not using this tool, already started with the driving licence in digital format as a means of identification, the next form will be this.

The key to this is to monitor this through the Digital Economy and Society Index (DESI).
They pursue a digital transformation that respects fundamental rights, data protection and non-discrimination by reinforcing all these aspects with change. And with the principles of technological neutrality, net neutrality and inclusiveness.

The foundations of the origin of this movement lie in the "Tallinn Declaration on eGovernment", the "Berlin Declaration on Digital Society and Value-Based Digital Government" where they announced the scope for all of this new current without forgetting the "Lisbon Declaration on Purposeful Digital Democracy" to serve as a reference to everyone who joins to develop these ideas, a sustainable movement will only be realised if we are all part of it.

Work towards a democratic framework for digital transformation and respect for citizens both online and offline in a safe and secure digital environment.

Ensure empowered and informed interaction with algorithms and Artificial Intelligence systems for the user in a way that does not jeopardise their privacy and health and implement safeguards to ensure this. Information provided in an objective, transparent and reliable manner. Freedom of debate on large platforms to channel avenues of expression in a democratic manner along with mitigating risks such as misinformation.
Digital legacy as the basis of everyone's online journey, with no voluntary sharing of information, requiring authorisation for sharing and full knowledge of how it will be used.

A direction of technological advancement guided by cooperation and feedback between governments and citizens for the creation and adaptation of measures that truly encourage this.

Striving to ameliorate recent problems such as the digital divide that arose in the COVID-19 pandemic aggravating between environments safe from web use and those that do not enjoy that opportunity. Along with the risks created in the wake of this rapid growth.

After defining the direction the European Union wants to take and all the measures it wants to implement. Let's take a look at the changes in force as a result of the Cambridge Analytica case and how it changes our privacy and in some ways our lives.

6. Regulations in the wake of the scandal

6.1 European Regulation

The regulatory framework in force since May 2018 in Europe GDPR (General Data Protection Regulation) implemented with the aim of increasing the protection of sensitive information of users belonging to the European Union.

There are certain exceptions for this information to be processed, some of them are: Explicit consent by the user, provided that such conduct is not prohibited by EU law itself, the processing of this data is necessary either for legal compliance or in the interests of the data subject, if the processing is carried out in a way that ensures legitimacy and safeguards for non-disclosure purposes, personal data in the public domain are made available for use, necessary for reasons of public interest involving the law of the Union or of the Member States, the relation of the data to preventive or occupational medicine for the purpose of a real assessment of the worker's capacities always under the supervision of a professional under previously established guarantees and conditions and for general purposes such as public health or archiving in the public interest to ensure protection and progress always safeguarding the rights and freedoms of the data subjects. By respecting these guidelines, more than decent conditions with respect to privacy policy can be ensured.

The need for change comes into play because of vulnerabilities but also because of the need to deal with an emerging concept in this debate on information, the IoT (Internet of Things). Systems with some software intelligence and internet connectivity that govern all aspects of our lives today, the worrying thing about these is their increasing integration from 500 million in 2003 to an estimated 14.5 billion in 2022, by 2025 it is estimated that 27 billion IoT devices will be connected. With so many devices

accessing the internet and so much information in circulation, control is needed in some form before it is too late and it gets out of control.

6.2 United States Regulation

We have previously examined the measures imposed in accordance with the European competent authority; it is now time to examine the measures applied in the region where the issue first surfaced and how they are addressing it.

We discussed the Federal Trade Commission's investigation into possible violations of a consent decree that has been in effect since 2011 and, more importantly, we emphasised how the United States' inadequate privacy law allowed Facebook and Cambridge Analytica to operate with perfect impunity. Following numerous Mark Zuckerberg hearings, they discovered the hints of this current legislation proposal, which involved the House and Senate Judiciary Committees as well as the Commerce Committees.

The primary goal was to address privacy and data policy. In 2018, laws appeared as a way to govern this privacy, with the Senators Richard Blumental and Ed Markley's teams' proposals being the most significant.

The Federal Trade Commission is required by the Consent Act (S.2639), also known as the "Customer Online Notification for Stopping Edge-Provider Network Transgressions," to protect consumers' privacy with regard to the online services they use.

This bill aims to tighten both the information flow and the information requirements of various players or companies involved in this type of activity by focusing on the explicit consent of users before platforms use, share, or sell their data as well as notifying the sale, collection, or sharing to a third party.

The Social Network Privacy and Consumer Rights Protection Act of 2018, sponsored by Senator Amy Klobuchar, which sets comparable restrictions to the CONSENT Act, is similar to this legislation and will be prosecuted by the Federal Trade Commission since it falls under its jurisdiction.

This great debate for the moment is no more than an initiative for change as the road to be resolved is long, but if the measures are carried out properly, it may be that the beginning in a State will be echoed and it will end up being imposed, the repercussions of this being positive for the privacy of users and the real value of the data, finally putting an end to manipulation and attacks on privacy.

The importance of this case is no more than the reality that it brought to the data ecosystem and how it reflected the loss of user power due to their lack of knowledge, as a service that they assumed to be free, apart from not being free because the price was their information, was also generating money at their expense.

One of the most famous phrases associated with this is that when a product is free it is probably because the product is you, which helped to raise awareness of people's behaviour on the internet.

This brought pressure from governments for Meta to increase its transparency and accountability about the advertisements that circulate on its platform, highlighting the way in which the information it provides is used by the companies to whom it is provided.

6.3 Developments in the courts

In April 2018 Mark Zuckerberg was summoned before the Senate of the Capitol in an appearance of more than 5 hours where he tried to justify himself in the face of the mistake made by his company and ended up recognising his error and apologising.
In the face of the strong accusations Cambridge Analytica ended up closing the business in May 2018 for reasons of chasing away suppliers and clients after the public accusations.

In May 2018 it also had an appearance in the European Parliament due to tensions with Europe and its data protection agencies.

This resulted in a fine of £500,000 and then a much more significant fine of $5 billion from the US Federal Trade Commission for its relationship with Cambridge Analytica and violating the Data Protection Act.

All the events mentioned above plus all those accumulated in different lines of action on the part of the company in question.

7. Conclusion:

As a final contribution to the information already presented, we will comment on some of the main reflections backed up by the arguments used, in order to clarify them.

We cannot overlook the dependence and need for social networks in the daily lives of a large part of the population, which is worrying because of the little benefit that people themselves obtain and how tremendously profitable they are for companies. Sometimes it is worth taking stock of whether these routines really contribute something or whether they are simply an unconscious action that we have automated. Systems designed for extremes, either you love it or you hate it, this type of company does not like the in-between, understandable since what sells most are these opposing stimuli. The dopamine that these generate is what makes us experience an engagement of this calibre to platforms that we don't really need for the development of our function.

Living in an ecosystem full of misinformation and violations of privacy rights has become commonplace, protected by lawlessness and inconsistent privacy policies. We have a very powerful tool in our hands but at what cost are we willing to use it, are we really focusing on it in the optimal way or are we just getting carried away. Of course not, we are capable of much more, which is why we are betting on a 'Sustainable Future' in the digital environment. We cannot lose any more ground than we have lost so far. After all that has come to light and seeing how they manipulate and misinfluenced by the holding of our data, there is no longer any option to remain impassive.

The measures continue to increase, trying to somehow regulate these large companies that concentrate so much information and power. Aiming towards a course where internet browsing is the responsibility of the user himself but with much more

favourable conditions and where the absorption of his information is under explicit consent, also limiting the areas that this information touches.

And even though the volume of business generated by practices associated with those carried out by Cambridge Analytica has now slowed down, many companies continue with this, such as Data Trust and i360, because as long as there is business, the activity will not cease.

Aware of what surrounds us, the best initiative to implement is to be careful, to be alert and not to trust in terms and conditions that assure things that they do not fulfil.

The best way to support sustainable development in technology is to be part of it, with interest and information. Build a community that lives up to the resources we have, no matter how good what we have at our disposal is, without a use that lives up to it, we completely lose its potential.

8.Bibliographical References

M. Fevzi Toksoy (2022). *Processing of Personal Data Inside Out: the Opinion of AG Rantos in C-252/21 (Meta Platforms v. Bundeskartellamt)*. [online] Kluwer Competition Law Blog.

France 24,(n.d.) (2022). *Mark Zuckerberg, demandado por la Fiscalía de Washington por el caso 'Cambridge Analytica'*.

Meta Business Help Center 2022. (n.d.). *About Advertising Restrictions*.

Dobinick, Susan. *Mark Zuckerberg and Facebook*. The Rosen Publishing Group, Inc, 2012.

Scanlan, E., Davis, P., Curtis, B. and Newman, B. (2022). *Censorship on Facebook BYU School of Communications COMMS 382: Global Issues in Communications*. pp. 2-8

Corbacho, J. (2020). *Facebook paga 500M de euros y pone fin a su juicio por usar sin permiso datos biométricos*.

Facebook (2021). *Advertising on Facebook*. [online] Facebook Business.

Company info: Meta. Company Info | Meta. (n.d.).

J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp. 56-59, August 2018, doi: 10.1109/MC.2018.3191268.

Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiseau, P. and Mislove, A. (2019). Measuring the Facebook Advertising Ecosystem. *Proceedings 2019 Network and Distributed System Security Symposium*.p 2-14. [online] doi:10.14722/ndss.2019.23280.

P. Barford, I. Canadi, D. Krushevskaja, Q. Ma, and S. Muthukrishnan, Adscape: Harvesting and analysing online display ads, 2014.

Berghel, Hal. Malice domestic: The Cambridge analytica dystopia. Computer, 2018, vol. 51, no 05, p. 84-89.

Misuraca, Gianluca, et al. Envisioning digital Europe 2030: scenarios for ICT in future governance and policy modelling. p.63-66. European Foresight Platform.–2012.–C, 2012, 632012.

J. G. Cabañas, A. Cuevas, and R. Cuevas, Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes, 479-485, 2018.

Perrin, Andrew. Americans are changing their relationship with Facebook p. 1-2. Pew Research Center, 2018, vol. 5

Perrin, A. J. (2019). *Civic hope: How ordinary americans keep democracy alive p 30-47*. Los Angeles, CA: Sage Publications, Inc. doi:10.1177/0094306119853809s

Boyd, Danah and Hargittai, E. (2010) “Facebook privacy settings: Who cares?”, First Monday, 15(8). p.1-1. doi: 10.5210/fm.v15i8.3086.

Anon, (n.d.). *772 millones de direcciones mail y 21 millones de contraseñas en MEGA, se destapa la mayor filtración de la historia*.

"Cambridge Analytica—The Power of Big Data and Psychographics" presentation Cambridge Analytica June 2016

Datta, A., Tschantz, M. C., & Datta, A. (2015). *Automated experiments on ad privacy settings.*p.1-26. Privacy Enhancing Technologies Symposium Advisory Board. doi:10.1515/popets-2015-0007

Godoy, J.D. (2020). Caso #3: Cambridge Analytica, la gran fuga de datos. El País. 16 Oct.

Álvaro Sánchez (2018). Zuckerberg pide perdón en la Eurocámara por el escándalo de la filtración de datos. EL PAÍS.

Barcelona, C.J. / (2017). *España multa a Facebook con 1,2 millones por recopilar datos sensibles de los usuarios sin permiso*.

European Union.(2022), European Declaration on Digital Rights and Principles for the Digital Decade.p 1-9

European Union.(2022), Communication from the Commission establishing a European Declaration on Digital Rights and Principles for the Digital Decade.p 1-7.