LUISS

Corso di Laurea in Data Science and Management

Cattedra: Privacy In the Digital World

Consent to Profiling in The Era of Data Science: Ethical Implications, Privacy Management, and Data Monetization in the Digital World.

Prof. Antonio Cilento
RELATORE

Prof. Massimo Chiriatti
CORRELATORE

Matr. 764061
CANDIDATO

Anno Accademico 2023/2024

Consent to Profiling in the Era of Data Science: Ethical Implications, Privacy Management, and Data Monetization in the Digital World.

Summary

Introduction.

Chapter 1: Contextualization of the Theme

1.1 The importance of profiling in the era of Data Science as a key phenomenon in the digital context

1.1.1 Overview of ethical, privacy, and data monetization issues in the context of profiling

1.2 Research Objectives.

1.2.1 Defining the main objectives of the thesis, focusing on the legal and contractual aspects of profiling.

1.2.2 The fundamental role of clarity on the ethical, privacy, and data monetization aspects to be examined, with a specific focus on contractual relationships related to consent for the use of cookies.

1.3 Research Methodology

Chapter 2: Profiling in the Age of Data Science

2.1 A specific focus on the interconnection of data science and profiling processes with privacy protection (Directive 2002/58/EC)

2.2 Ethical and Legal Implications of Profiling.

2.2.1 In-depth analysis of the ethical risks and legal implications associated with the collection and analysis of personal data.

2.3 Privacy Management in Profiling (cookies)

- Role of privacy laws and regulations in the legal context of profiling

- Legal techniques and strategies to ensure privacy protection during profiling, with a focus on contractual aspects in cookie consent

Chapter 3: Monetizing Data in the Digital World.

3.1 Business Models Based on Profiling.

3.1.1 Legal analysis of business models that leverage data profiling, highlighting applicable regulations and laws.

3.1.2 Economic benefits and associated critical issues from a legal perspective.

3.2 Balancing Profit and Social Responsibility.

3.2.1 Legal strategies for a sustainable approach to data monetization, including specific contractual tools.

Chapter 4: Case Study - Facebook

4.1 Facebook Company Profile.

- Brief presentation of the company and its role in profiling, with a legal perspective

4.2 Facebook Profiling Practices.

- Legal analysis of profiling practices implemented by Facebook highlighting critical issues in the case study.

4.3 Ethical and Privacy Implications in the Facebook Case.

- Legal assessment of ethical implications and privacy issues in the context of Facebook

- Analysis of Facebook's responses to the concerns raised from a legal perspective

4.4 Conclusions from the Facebook Case

- Lessons learned and broader implications for the digital world, with a specific focus on legal

4.5 Summary of Key Findings.

- Summary of key findings that emerged from the research, with an emphasis on legal aspects

Bibliography

Introduction

In the contemporary digital landscape, the interplay between Data Science and user profiling has increasingly become a pivotal force, shaping the way individuals, businesses, and societies interact with information, and, within the context of Data Science, goes beyond mere data analysis; it extends to ethical considerations, privacy management, and the complex concerns regarding data monetization.

Therefore, this thesis analyzes the intricate theme of consent to profiling in the era of Data Science, embarking on a comprehensive journey that explores collateral arguments related to it, as its ethical implications, privacy management intricacies, and the legal aspects surrounding data monetization in the digital world.

With the aim of doing so, a real case study will be proposed to highlight the crucial facets through a more practical approach: The Facebook Case, which serves as an excellent real-world example of the cruciality of the theme that is being analyzed.

The first chapter focuses on establishing a foundational understanding of the importance of profiling in the era of Data Science within the digital context. As a matter of fact, it first aims to underscore the fundamental role that profiling assumes in the contemporary landscape, studying profiling as a key phenomenon in shaping the digital landscape and influencing numerous aspects of data-driven decision-making. It consequently starts to introduce the ethical considerations and privacy concerns that must be addressed, designing the appropriate space for a deeper understanding of the interconnected issues, and for a thorough introduction of the research objectives.

The second chapter engages the intricate relationship between Data Science and profiling, with specific attention to privacy considerations and legal concerns. More specifically, it debuts by showing the interplay between Data Science and Profiling processes, with a specific focus on Directive 2002/58/EC, to outline the connection with privacy protection. Furthermore, the chapter proceeds by outlining both the ethical and legal implications connected to profiling, providing an in-depth analysis of the risks associated with profiling, as well as examining the specific legal considerations tied to the practice of profiling, addressing the regulatory landscape and legal implications surrounding the collection and analysis of personal data, bridging the gap between theoretical knowledge and practical applications. Finally, the legal techniques and strategies employed to ensure privacy protection in the profiling process are investigated, particularly highlighting contractual aspects in the realm of cookie consent.

The third chapter delves into the complexities of data monetization with a specific focus on business models built upon profiling. The chapter aims to provide a legal perspective on the associated regulations, economic benefits, challenges in balancing profit with social responsibility, and sustainable approaches to data monetization. As a matter of fact, it starts by conducting an analysis, from a legal point of view, of the business models leveraging from it, shedding a light on the legal frameworks that govern business models based on profiling, offering insights into economic benefits, challenges, and strategies, to achieve a sustainable and responsible approach to data monetization. Finally, in this chapter, we will emphasize the specific contractual tools designed to align profit-seeking with ethical and social considerations.

The fourth chapter serves as a detailed examination of a prominent case study, offering a real-world perspective and illustration of the legal, ethical, and privacy aspects associated with profiling practices. Particularly it will focus on the Facebook case and its role in this complex context. More specifically it will focus on three fundamental aspects of the matter: the analysis, from a legal point of view of the profiling practices implemented by Facebook; a deeper assessment of the legal and ethical implications and Privacy issues associated with Facebook's profiling practices, and, finally, the response of the platform to the concerns raised will be analyzed.

Chapter 1: Contextualization of the Theme

1. The importance of profiling in the era of Data Science as a key phenomenon in the digital context

From a literal perspective, profiling is defined as the act or process of extracting a person's information based on known traits or tendencies, [1] However, this term gains a more intricate meaning when contextualized in the Data Science framework.
As a matter of fact, it is fundamental, to achieve a holistic view of the topic, to circumscribe and define the three main actors involved: Data subject, data controller, and data processor.

- Data Subject: a natural person who can be identified, either directly or indirectly, whose personal data is being analyzed or processed to create profiles or predictions about them. [2]
- Data Controller: is the actor whose objective is to determine whether the profiling activities will be conducted, and if so, which data will be used and for what purpose.
- Data Processor: is a separate entity that processes personal data on behalf of the data controller, acting according to the instructions given by it. In the context of data science, a data processor might be a third-party service or software. [3]

The three subjects mentioned above, as can be seen, all have a specific role in profiling, which, as defined in Art. 4 of the GDPR, is any automated processing of personal data, consisting of the utilization of the aforementioned to evaluate specific attributes regarding the natural person, more specifically with the scope of extracting insights and predicting their interests and behavior. [4]

After introducing the theoretical concept, it is therefore imperative to expound upon the significance of profiling in the era of Data Science and its diverse spheres of application.
As a matter of fact, profiling enables the analysis and interpretation of complex data patterns by leveraging advanced Machine Learning algorithms techniques, which facilitate the identification of valuable and meaningful correlations and predictive models, thereby empowering decision-making processes across diverse domains.

1. Profiling. (2024b). In *Merriam-Webster Dictionary*.
2. Data controller or data processor | European Data Protection Board. (n.d.).
3. Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR). (2018, March 29). General Data Protection Regulation (GDPR).
4. Altalex, R. (2019, January 24). Art. 4 GDPR - definizioni. Altalex.

One of the crucial and most valuable outcomes of profiling lies in its ability to enhance customization in various sectors, including marketing, healthcare, finance, and beyond. In

marketing, for instance, profiling enables crucial features for businesses such as segmenting their target audience effectively, tailoring marketing strategies, and delivering personalized content or recommendations to individual consumers.

As a matter of fact, profiling serves as a cornerstone of Data Science, driving insights, innovation, and decision-making across a wide range of applications. Therefore, its ability to gain meaningful information from datasets, and enhance personalization underscores its critical importance in the digital age.

1.1 Overview of ethical, privacy, and data monetization issues in the context of profiling

In the continuously evolving landscape of Data Science, the practice of customer profiling has become increasingly pervasive, offering businesses meaningful insights into consumer behavior and preferences.
However, the adoption of profiling techniques, despite the numerous valuable benefits, also raises ethical concerns, privacy implications, and questions surrounding data monetization strategies.

When analyzing the outcomes, and areas of impact of profiling, it is fundamental to also consider the ethical concerns that arise from the potential misuse, exploitation, or malicious behavior behind the use of customer data in the process of profiling. One of the primary ethical considerations that must be addressed is the obligation of businesses to ensure transparency and fairness in their profiling practices, which includes providing the Data Subject with clear information about the collection and use of their data, and equally important, is to obtain informed consent for the data processing activities.
Moreover, continuing the analysis from the standpoint of ethical considerations, it is important to also address the potential biases inherent in profiling algorithms, which may perpetuate discrimination or unfair treatment toward certain demographic groups, which leads to the need to establish and apply ethical frameworks and guidelines to mitigate these biases and ensure that data processing activities uphold principles of fairness, equity, and respect for individual autonomy.[5]

5. Rana, J. (2023, May 26). Customer profiling. Mike Vestil.

Additionally, given the sensitive nature, as well as the vastity, of the personal data involved, privacy concerns are paramount in the context of customer profiling, in fact, businesses must address and be

aware of the heightened risk of privacy breaches and unauthorized access to sensitive information for malicious purposes or unauthorized disclosure.[6]

In order to safeguard privacy rights, robust data protection measures must be implemented, including encryption, access controls, and regularly conducting security audits. Additionally, compliance with privacy regulations such as the General Data Protection Regulation (GDPR), is essential to ensure a lawful and ethical handling of the customer's data. [7]

Finally, an equally important matter that must be addressed is that businesses, in the pursuit of profit and competitive advantage, may consider monetizing the customer data obtained through profiling activities.

The term 'Data monetization' consists of the transformation of data into direct profits either for companies or for individuals, through the fruition of digital content or services using data as compensation. This process can also occur by selling data, offering targeted services, or additional commercial initiatives revolving around data; from this concept stems the innovative bridge that links data to direct profits. An interesting practical example of the phenomenon is the practice employed by social media platforms, which collect vast amounts of data thanks to the interaction with the platform, including likes, comments, and demographic information, to allow advertisers to target the right audience, for data analytics purposes, and for data sharing agreements with third-party companies, allowing the disclosure of data in exchange of profitable revenues, or enhanced services.

However, this concept raises significant ethical questions regarding the commodification of sensitive information such as personal data, and the extent to which individuals should have control over the monetization of their data.[8]

In fact, although data monetization can offer substantial economic benefits for businesses, they must also consider respect for individual privacy and ethical considerations.

As a matter of fact, it is fundamental the adoption of transparent data monetization practices, providing customers with clear information about how their data is being used, shared, and monetized.[9]

6. Profiling the Mobile Customer –
   Privacy Concerns When Behavioural Advertisers Target Mobile Phones – Part I
7. Secure personal data | European Data Protection Board. (n.d.).
8. Boccaccini, P., Torresan, C., Boccaccini, P., Torresan, C., Boccaccini, P., & Torresan, C. (2023b, September 20). Data valorization e data monetization, il dato quale asset strategico per il business: le sfide future. Cyber Security 360.
9. Writer, G. (2023, September 4). The ethics of data monetisation: Balancing personal privacy with economic value | TheCable.

1.2 Research Objectives.

1.2.1 Defining the main objectives of the thesis, focusing on the legal and contractual aspects of profiling.

The primary objective of the thesis is to provide a comprehensive analysis and understanding of the multifaceted landscape of profiling, with a specific emphasis on the legal and contractual standpoints.

The objective within this scope includes delving into the legal frameworks and regulatory landscape governing profiling activities which comprehends scrutinizing laws regarding the matter, directives, and guidelines pertinent to data protection, privacy rights, and consumer consent.

Moreover, the aim would be to assess the legal rights and obligations of both individuals and entities involved in profiling activities, which entails the investigation of the legal principles revolving around data processing, including consent, purpose limitation, and transparency towards the data subjects regarding the purpose of the processing activities, as well as the different subjects that will be provided with access to the data collected. Among these last themes cited it would be important to provide peculiar attention to the theme of consent due to its direct link with different topics such as clarity and transparency, which will be later discussed and deeply analyzed.

Additionally, the objective of the text lies in the identification of potential legal risks associated with profiling activities and proposing effective and efficient compliance strategies, including the analysis of possible complications such as data breaches, legal liabilities, practices that are non-compliance with regulations, and offering recommendations and best practices for risk mitigation purposes.

Finally, within this context, the aim will be to explore the contractual frameworks and synthesize the legal perspective. As a matter of fact, the thesis will explore and delve into the contractual frameworks governing profiling practices, with a specific focus on the contractual relationship that links data subjects, data controllers, and third parties, which includes examining the role of contracts, of the terms of service, the privacy policies, and consent mechanisms in transforming the landscape of profiling. Legal precedents, case law, and emerging legal trends will also be included to gain a tangible perspective of the theoretical aspects.

1.2.2 The fundamental role of clarity on the ethical, privacy, and data monetization aspects to be examined, with a specific focus on contractual relationships related to consent for the use of cookies.

In addition to the specific focus on the legal and contractual aspects, as previously outlined, this thesis also aims to delve into the ethical, privacy, and data monetization dimensions of profiling, to emphasize the fundamental role of clarity in these areas.
Therefore, the research objectives within this scope belong to four macro-areas: an examination of ethical considerations, an analysis of privacy concerns, an assessment of data monetization strategies, and an emphasis on contractual relationships and consent mechanisms.

Specifically, this thesis, due to the sensitive nature of the personal information that is mostly collected to conduct profiling activities, focuses on managing a critical examination of the ethical implications involved, particularly considering the individual's autonomy, principles of fairness, and societal implications. This involves the assessment of ethical frameworks and guidelines pertinent to profiling practices, as well as evaluating the ethical responsibilities of stakeholders involved, to provide a homogenous reference that will largely, and for the most part, grant ethical and face profiling activities.

Secondly, the focus is directed to the analysis of privacy concerns that arise from profiling, specifically focusing on data collection, processing, and sharing practices. This includes evaluating the impact of profiling on individuals' right to privacy, autonomy, and dignity, as well as considering measures to enhance privacy protection standards.

Thirdly, the objectives include the assessment of data monetization strategies utilized in profiling practices, including targeted advertising, data brokerage, and personalized marketing, which entails examining the economic incentives driving data monetization, as well as complications related to the risks and benefits stemming from ethical, privacy, and legal perspectives.

Finally, in order to highlight the importance of clarity in the fundamental contractual relationships that stem from the consent for the use of cookies and other tracking technologies employed to conduct profiling activities, the transparency of the use of the data collected the adequacy of the procedures, and the effectiveness of consent mechanisms employed by data controllers are

analyzed, additionally, proposes to enhance the safety of informed and meaningful consent are proposed.

By taking into consideration these objectives, and carefully addressing them, this thesis aims to contribute to a nuanced understanding of profiling in the digital age, while offering insights and recommendations for the promotion of ethical legal, and transparent practices in this continuously evolving landscape. As a matter of fact, through a holistic approach, this research seeks to foster clarity and accountability in profiling activities, to promote homogenous ethical, and privacy standards, and lawful practices, to protect and safeguard data subjects from malicious behaviors and privacy disruption.

1.2Research Methodology

The purpose of this section is to outline the methodology utilized for conducting thorough research on the legal and contractual aspects of profiling in the era of Data Science. Through the methodology employed, the aim is to provide a systematic approach to address and analyze the objectives that have been previously set forth.

The research methodology begins by setting an extensive literature review, encompassing scientific and updated articles, conference papers, and official documents relevant to profiling in the digital context, by doing so the aim is to form the foundational knowledge base for the research, as it facilities the identification of gaps existing in literature, highlighting the common grounds and most relevant, and sensitive topics, and informing subsequent stages of study.
Additionally, conducting a comprehensive literature review allows the employment of comparative studies between legal frameworks, regulatory approaches, and enforcement mechanisms across different jurisdictions, which allows the identification of the factors influencing the effectiveness of legal regulation in addressing emerging challenges posed by technological advancements.

Following the literature review, a holistic analysis and comprehension of the legal and contractual topics is conducted, in order to examine relevant statutes, directives, regulations, case law, and juridical interpretations of profiling and data science. Additionally, a scrutinization of the key legal frameworks, mainly the General Data Protection Regulation, and Directive 2002/58/EC (ePrivacy Directive) will be conducted in this thesis, in order to understand their implications and impacts on profiling practices, privacy protection, and data monetization activities. Through the

aforementioned legal analysis, the aim is to elucidate legal obligations, rights, responsibilities, and possible liabilities linked to profiling activities, setting the proper space for a deeper understanding of the legal landscape.

The methodology entails the analysis of real-world case studies such as the ‘Facebook case’ to provide practical insights into the legal and contractual aspects of profiling. The mentioned case study has been selected based on principles of relevance, considering aspects such as representativeness, impact on the sector and the industry, as well as on the data subjects involved. Through a qualitative analysis, the thesis examines the factual circumstances that made the specific case relevant to the current landscape, the legal argument, the ethical dilemmas that had an impact on the data subjects, and the societal effects.

Lastly, the research methodology focuses on addressing the ethical considerations in all stages of the research process, guided by relevant principles such as respect for an individual’s autonomy, justice, malicious or non-malicious behavior, and integrity.
The main focus regarding this intricate topic is on the power dynamics and cultural sensitivities inherent in profiling practices, striving to minimize harm and maximize ethical conduct.

By integrating these methodological components, the thesis adopts a holistic and interdisciplinary approach, investigating legal and contractual aspects concerning profiling, as well as the ethical and security best practices. Through this methodology, the aim is to facilitate the generation of robust empirical evidence, the development and improved understanding of nuanced theoretical insights, and the formulation of practical recommendations for industry stakeholders.

Chapter 2: Profiling in the Age of Data Science

2.1 A specific focus on the interconnection of data science and profiling processes with privacy protection (Directive 2002/58/EC)

In the contemporary digital landscape, the interplay between Data Science and Profiling processes is a central phenomenon with profound implications, particularly concerning privacy protection matters. Specifically, Directive 2002/58/EC, commonly known as the "ePrivacy Directive", assumes a fundamental role in defining the parameters and the area within which such practices operate while ensuring the protection of the individual's rights to privacy and data protection within the European Union.

At its core, Directive 2002/58/EC is a cornerstone of privacy legislation, specifically addressing electronic communications and the processing of personal data. It outlines a comprehensive framework with the specific objective of ensuring the appropriate confidentiality of electronic communications, and more importantly for our purpose, aligning closely with broader principles of Data Protection enshrined in the EU Charter of Fundamental Rights and the General Data Protection Regulation (GDPR). [10]

As previously anticipated, within the realm of Data Science and Profiling, the interplay between technological advancements and privacy concerns is a matter of particular interest. As a matter of fact, profiling intended as the automated processing of personal data to evaluate specific personal aspects, often entails the aggregation and analysis of vast datasets to generate predictive insights or ad-hoc marketing strategies, therefore leading to important benefits as well as raising concerns that are inherent in this practice, mainly regarding privacy infringement and data misuse.[11]

To this end, Directive 2002/58/EC addresses these concerns by defining stringent guidelines and obligations on Member States to safeguard individuals' right to privacy and data protection in electronic communications, granting data subjects specific rights pertaining to the processing of their personal data, including the right to be informed about the processing, the right to opt-out of certain types of processing, and the right to confidentiality of communications.[12]

Furthermore, the Directive outlines explicit requirements for obtaining valid consent for the use of

10. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058
11. https://link.springer.com/article/10.1007/s11301-022-00309-1
12. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

tracking technologies such as cookies, which are integral to many profiling activities.
As a matter of fact, organizations must provide users with transparent information about the use of cookies, defining their purposes and clearly outlining the possibility of opting out, as well as the options available to manage cookie preferences, additionally, it is important to consider the fact that emphasizing transparency and user control reflects the directive's overarching goal of empowering individuals to make informed choices about their data, ensuring the user's freedom of choice regarding the use of their personal data as well as their right to their privacy to be preserved and protected.

In practice, compliance with Directive 2002/58/EC is paramount for organizations engaged in profiling activities, as it allows the lawful and ethical processing of personal data while maintaining an individual's fundamental rights.
By adhering to the principles and requirements outlined in the directive, organizations can build trust and confidence among users, fostering a culture of responsible data practices and privacy protection in the digital age.

2.2 Ethical and Legal Implications of Profiling.

Profiling has currently assumed a vital role in the conduction of contemporary data-driven practices. However, it comprehends significant ethical and legal implications related to the collection and analysis of personal data that must be addressed, analyzed, and considered by the stakeholders involved, in order not to risk undesired outcomes such as limitation of privacy and freedom of choice of the data subjects.

As a matter of fact, in the attempt to explore the ethical landscape of profiling, it is evident that beyond concerns of privacy infringement and bias, there is a deeper dilemma stemming from the commodification of personal data that must be addressed. Therefore, this section delves into the intricate interplay between data ownership, consent, and individual agency, unearthing the ethical tensions arising from the commercialization of personal information and its impact on societal values and norms.

In addition to that, the legal aspects related to profiling extend their domain beyond mere compliance with regulatory frameworks, affecting emerging intricate legal concepts such as data sovereignty and the accountability of the algorithms, therefore the aim of the thesis in this section would be to examine the evolving jurisprudence surrounding data rights and responsibilities.

2.2.1 In-depth analysis of the ethical risks and legal implications associated with the collection and analysis of personal data.

The collection and analysis of personal data are often, correctly, associated with the benefits it conducts to businesses and how they can make their decision-making process more effective and efficient. Despite the factual improvements that are observed in businesses that utilize these useful tools, several collateral effects must be considered as they should be given equal importance. The streams that are going to be followed are the following: the ethical and legal concerns related to it. Starting the in-depth analysis with the first stream, the concept branches out to various sub-arguments.

Starting from the Privacy Concerns, data subjects often claim that privacy should be protected, failing to precisely translate what this concept means to them, paving the way to an argument that should be considered: clarity. As a matter of fact, because legislators and judges find it difficult to express the privacy harm, this lack of clarity causes problems when drafting legislation or deciding legal disputes, in fact, privacy interests are often overlooked by courts and legislators, which results in cases being dismissed or laws not being passed. As a result, competing interests are not considered when weighing privacy. While, from a more ethical perspective, which is the stream of focus for the moment, this section will focus on the paper of Daniel J. Solove, in "A Taxonomy of Privacy", in which the author presents a comprehensive framework to provide a conceptual framework that helps the understanding of the ethical complexities inherent in protection of privacy rights in the digital age.

Based on the broader themes discussed in Soloves's paper, it is possible to recognize several ethical concerns related to privacy. As a matter of fact, the paper starts by exploring how privacy can be invaded through different ways of data processing, making a distinction between, surveillance, data collection, and information dissemination. Ethical concerns are in fact raised when individuals' personal information is accessed, used, or shared without their consent, potentially leading to harm or limitation of the data subject's autonomy. Successively, the ethical implications of data misuse and abuse are a critical matter in the case in which the information is exploited for purposes that go beyond the originally ideated purpose without proper communication and safeguards, as it may lead to improper use of data due to privacy breaches, identity theft, and several additional forms of harm to individuals. Moreover, it is fundamental to take into consideration the fact that individuals have the right to transparency regarding how their data is being collected, used, and who has access to it, without the proper information individuals may lack the knowledge of the potential risks regarding

their privacy. Finally, Solove discusses an incredibly delicate topic regarding data processing, which is the ethical issue revolving around discrimination and profiling based on personal data. As a matter of fact, it is discussed how much attention Data Processors and Data Controllers should give when using personal information, as by categorizing individuals or by deciding between them, there might be a high risk of biases and inequalities, leading to unfair treatment and discrimination.[13]

Additionally, it is crucial, relatively to the topic of ethical concerns, to address the matter of Informed consent. As a matter of fact, it includes the certainty that individuals have thoroughly understood how their data will be utilized and the potential risks stemming from it, allowing a voluntary, conscious, and informed decision regarding the use of their personal information.

The theme of Informed Consent entails the issues revolving around PIIs (Personally Identifiable Information). In fact, often companies apply criticisable practices by ensuring customers that, after the de-identification of data they may be safely released without further risks, as they would not have direct links that would allow the re-identification. However, this assumption does not take into consideration the intricacies stemming from data re-identification, raising ethical issues and questions regarding the adequacy of an individual's understanding and consent, and lacking the fundamental principle of transparency required when discussing the delicate topic of data processing. As a matter of fact, the topic of re-identification leads to an even more intricate and delicate topic which is the need to prioritize privacy as a fundamental human right, as well as protecting the data subject's sensitive information from unauthorized disclosure.[14]

Relatively to the legal implications associated with the processing of personal data, it may be beneficial to discuss some of the topics entailed in Article 29 Data Protection Working Party's "Guidelines on Consent under Regulation 2016/679", as it provides detailed parameters on the application of consent requirements under the General Data Protection Regulation (GDPR).

13. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-560.
14. Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information". Communications of the ACM, 53(6), 24-26.

Specifically, the guideline provides a clear and thorough explanation of the situations in which explicit consent is required, both for a matter of the sensitivity of the data and of the sensitivity of the data subject. For example, the cases in which the data that is being processed contains personal information or the cases in which the person whose data is being processed is a minor. Additionally, the right of revocation of consent is analyzed, specifically regarding the instructions for the implementation of mechanisms that may facilitate the subject's withdrawal of consent, even by providing easily accessible opt-out options. Finally, the topic of Third-party consent is taken into consideration as it allows a proper space of reasoning for the importance of ensuring transparency and accountability in multi-party data processing arrangements, including the right of the data subjects to be provided with clear information about the involvement of third parties and to be aware of the sharing and processing practices regarding their data.

Delving into a deeper analysis of the previously cited topics, starting from the particular attention required for data categories that require explicit consent due to their nature.
As a matter of fact, sensitive categories of data, including health information, genetic data, and biometric data, require that the data subject is fully informed about the collection, use, and sharing of their sensitive information, to allow a proper exercise of control.
For example, the processing of genetic data (meaning information derived from DNA, RNA, or genetic markers, may reveal details about their hereditary traits, susceptibility to diseases, and familial relationships. As a matter of fact, processing this specific category of data requires explicit and continuous consent, as it raises important ethical concerns regarding genetic privacy, which may lead to potential stigmatization, discrimination in employment or insurance, and unauthorized use for purposes that are not related to healthcare or scientific research.
This ethical concern is also directly linked to the legal importance of declaring the purpose of the processing, which cannot, under any circumstance, differ from the one agreed contemporarily to the moment in which the data subject gave explicit consent.

Moreover, in the attempt to provide specific details for the topic covered by the cited guidelines, relatively to the fundamental topic of revocation of consents, it is important for Data Controllers should provide clear and easy opt-out options to withdraw the consent given. As a matter of fact, as previously outlined, the consent must be continuous throughout the process, which may mean including mechanisms such as preference management tools on websites, or even dedicated consent withdrawal forms, at any rate, it is important for the means used for the purpose to be easily used, intuitive and accessible. Data Controllers should establish internalized procedures that can promptly

acknowledge receipt of the withdrawal of consent confirming the action, rapidly cease the processing of activities associated with the withdrawn consent as soon as possible, anonymize and delete relevant data, and refrain from further collection or use.
However, in specific cases in which data processing activities have already been undertaken, data controllers should evaluate whether is possible to continue the processing under alternative legal bases, such as for legitimate interests or legal obligations. In cases in which these circumstances are not present, data controllers must cease processing the data and take the necessary steps to mitigate any adverse effects on data subjects.[15]

Finally, to cover the relevant topics provided by the guidelines, it is important to consider the topic of Third-party consent, which is fundamental for building trust between data subjects and regulatory authorities.
In order to comprehend the logical connection aforementioned, it is important to understand the figure represented by the third party. GDPR defines it as "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.*"[16]
Although a formal similarity exists with the one of data processors, there is a key, substantial difference: a third-party does not process data on behalf of the data controller, instead they receive the data and are authorized to process it as they prefer, even by setting their own purpose and use it for their interest. This topic raises relevant concerns for data subjects, that we will delve into.
Data Controllers should establish contractual agreements, such as DPAs (Data Processing Agreements) with third-party data processors to gain a clear definition of each party's rights and obligations regarding data protection and regulatory compliance they must adhere to, confidentiality requirements, and specific obligations of data breach notification.
Specifically, regarding the obligations entailed, the data controller must ensure transparency and accountability in multi-party data processing agreements by informing, the individual, whose data is being processed, about the involvement of third parties, their specific roles, the purpose of sharing data, and the legal basis that allows the disclosure.

15. Article 29 Data Protection Working Party. (2018). Guidelines on consent under Regulation 2016/679(WP259)
16. Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR). (2018, March 29). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-4-gdpr/

Evidently, data subjects also have the right to be informed about their right to withdraw their consent, request access to their data, and lodge complaints with data protection authorities in case of believed malpractices. Lastly, before including third-party data processors, especially in high-risk processing, there is a fundamental step that data processors should conduct DPIAs (Data Protection Impact Assessments), in order to assess and mitigate the potential risks that may affect the data subject's rights and freedom as to enable the implementation of appropriate measures to allow the protection of personal data and ensure compliance with data protection laws.[17]

2.3 Privacy Management in Profiling (Cookies)

In the digital era, cookies, small text files that allow the recognition of the user's preferences and activities, that websites place on the user's device when they visit the site, have gained a particularly relevant role thanks to their polyhedric facets. Cookies serve various purposes, including:

- Session Management which represents the ability to store information about the user's session, allowing more efficient navigation by granting access to secure areas of the site without the need to re-enter the credentials.
- Personalization which allows the website to save the user's preferences, for example regarding the set language or specific customized layouts, to enhance the browsing experience.
- Tracking, as several cookies track user's behavior across websites to provide targeted advertisement. They are seldom referred to as tracking or third-party cookies as they are set by domains that differ from the one being visited.[18]

It is vital to remember, that while cookies may enhance the user's experience and website functionality, they can also raise serious issues related to privacy, especially when it comes to tracking cookies, because of the gathering and distribution of user data among websites that characterize their functionality. As a result, a lot of countries require that websites gather the data subject's permission before storing specific kinds of cookies, notably those that are used for tracking.

17. Article 29 Data Protection Working Party. (2018). Guidelines on consent under Regulation 2016/679(WP259)
18. *Use of Cookies*; Scientific American.

As a matter of fact, laws and regulations play a crucial role in governing the legal aspects of profiling, particularly referring to the use of cookies for tracking and profiling purposes. Particularly, the guidelines provided by the GDPR impose strict requirements on the collection and processing of personal data gained through cookies. In fact, it is expected for cookie consent, which must be freely given, unambiguous, and specific, to be obtained before placing non-essential cookies on the target devices, in this regard, users must thoroughly understand the purpose, the types of cookies used, and the duration of data retention.[19]

Additionally, e-Privacy Directive, which complements the GDPR, is a fundamental tool for the delineation of the perimeter that regulates the use of cookies and similar tracking technologies, it contributes to the creation of a proper environment that is both fruitful for data controllers and a safe for data subjects. Specifically, it entails specific cases in which certain tracking tools are necessary for the correction functioning of websites, including authentication, session management, and security safeguarding purposes. Lastly, the Directive includes two additional topics: transparency obligations regarding the kind of cookies used, the duration of the storage, and how can users manage their cookie preferences; and Penalties for malpractices enforced by national Data Protection Authorities in member states, in fact, in case of non-compliance with the requirements expected may result in sanctions and heavy fines. [20]

In the broad environment of the role of Privacy Laws and Regulations in the Legal Context of Cookie Profiling, the contractual aspects, which include an agreement between data controllers, data processors, and third-party service providers, are extremely delicate, although often underestimated. The purpose is to create the proper space for managing data processing activities and ensure proper compliance with privacy laws. Additionally to the contractual aspects that have previously been mentioned, three topics are considered relevant to the topic: Data Processing Agreements (DPAs), Indemnification and Liability**,** and International Data Transfers.

Data Processing Agreements gain relevance as they define the area containing the terms and conditions governing the processing of personal data, including the obligations of the data controllers and data processors, who are required to stipulate the agreement.

Secondly, contracts may contain specific clauses regarding the liability and indemnity as a

19. IAPP Cookie Consent Toolkit: International Association of Privacy Professionals (IAPP) toolkit for implementing cookie consent mechanisms and ensuring compliance with privacy regulations.
20. *Directive - 2002/58 - EN - eprivacy Directive - EUR-Lex*.

Consequence of data breaches or broken privacy laws and regulations by Data Processors or different third-party service providers which may be asked to indemnify data controllers for possible damages resulting from infringement of data protection laws pertaining to cookies.[21]

Lastly, the matter of transferring personal data obtained through cookies to third countries, excluded from the European Economic Area, expects specific contractual clauses or agreements that may be necessary to ensure adequate protection of the data that is being transferred, in agreement with the requirement previsioned by the GDPR. As a matter of fact, the transfers are only permitted under strict conditions, including the consent of data subjects and the mandatory necessity of the transfer for the performance of a contract. Specifically, the European Commission should issue Adequacy Decisions in order to confirm that the data protection laws expected in the country taken into consideration provide an adequate level of safeguarding that meets the standard of the GDPR; in such cases, if all the requirements are met, there will be no need for additional safeguards for data being transferred to that country. As a matter of fact, if the country where the data is being transferred does not meet the standard requirements, data controllers can implement pre-approved contractual clauses established by the European Commission, called Standard Contractual Clauses; which impose strict and monitored data protection measures both for the data exporter, which is the data controller and the data importer, which is the data processor. [22]

Thanks to the implementation of the requirements mentioned and the specific contractual aspects, it is possible to maximize the safety of personal data tracked using cookies, while maintaining a fruitful ground for data controllers.

Chapter 3: Monetizing Data in the Digital World.

3.1 Business Models Based on Profiling.

Business models based on profiling have assumed a significant role in the contemporary economic landscape, mainly due to the fundamental role played by the collection and analysis of user data in shaping commercial strategies and services. Profiling, within this context, refers to the activity directed to the identification of user profiles by collecting and analyzing large volumes of data through the asylum of sophisticated algorithms that allow the extraction of valuable insights,

21. *Cookies | Legals | Leonardo3*. (n.d.). https://www.leonardo3.net/en/legals/cookies/
22. International data transfers | European Data Protection Board. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

which are subsequentially utilized for various purposes such as targeted advertising, and personalized recommendations, which are usually beneficial for the data controller, but may also facilitate the user's navigation and increase their experience thanks to the ability to obtain personalized content.

Additionally to the shaping of commercial strategies, it is fundamental to take into consideration the fundamental role played by data monetization in profiling-based business models. Specifically, data monetization refers to the practice of generating either revenue or economic value from users' data through various means which can be either a direct source of revenue, such as Targeted advertising, or indirect such as data licensing and the establishment of partnerships with third-party entities.[23]

As aforementioned, data monetization and profiling are currently shaping the digital economy's landscape, as a matter of fact, it is being employed by several business models for the generation of additional revenue streams. One of the main examples of this change is extensively provided by Social Media Platforms, which allow advertisers to reach specifically targeted demographics. Additionally, social media platforms may also establish data licensing agreements, which include selling anonymized data to third-party entities, which will be used for different purposes, such as market research and advertising targeting.

As a matter of fact, it is evident how, although the primary focus of these business models would be to deliver a customized and enhanced experience, they also capitalize on the incredibly important value of user data by employing data monetization strategies to generate additional revenue streams.[24] This aspect is fundamental for the subsequent analysis of the contractual aspects concerning the topic and the protection of the data subjects' rights to have control of their data.

3.1.1 Legal analysis of business models that leverage data profiling, highlighting applicable regulations and laws.

Depending on specific characteristics such as demographic positioning and the industry in which they operate in, different laws and regulations can affect businesses that leverage data profiling. As a matter of fact, it is fundamental for such companies to ensure compliance with those mentioned above, to avoid extremely relevant legal consequences such as fines and lawsuits, and, most importantly for the market, reputational damage.

23. Mayer-Schönberger, V., & Ramge, T. (2018). Reinventing capitalism in the age of big data. Basic Books.
24. Turow, J., Hennessy, M., & Draper, N. (2015). The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation. Annenberg School for Communication at the University of Pennsylvania.

Relatively to the latter, in order to build trust with consumers and demonstrate accountability for data-handling practices, it is fundamental for businesses to ensure transparency regarding both the purpose and the safety of the practice, as well as who will receive the collected data.

This concept is linked to the matter of data security, as the protection of the confidentiality and integrity of personal data is fundamental to mitigating the risk of data breaches, as well as upholding individual privacy rights, which are significant topics for the appropriate compliance of such business models to laws, as well as for their credibility in the market.

Delving into the specific applicable laws and regulations that must be followed, each of them regarding business models that have specific characteristics, it is of relevance the set of data privacy and data protection regulations that concerns any company that collects or processes personal data of individuals residing In the European Union: The General Data Protection Regulation (GDPR). The latter aims to strengthen and align data protection laws across member states and provides rigid requirements, many of which have already been thoroughly explained, such as consent, the right of the data subject to access, and rectification, as well as two additionally important topics, which are the right to erasure, and the provisions regarding data protection by design and data protection by default.

Firstly, the right to erasure is a specific provision entailed in the GDPR, which is also known as the "right to be forgotten", that determines the right for the data subject to get their data deleted under specific circumstances, such as unlawful processing, the cases in which data is no longer necessary for the purpose previously declared by the company, compliance with a legal obligation EU or member state law to which the data controller is subject.[25]

Secondly, in order to conduct a thorough legal analysis of business models that leverage data profiling it is fundamental to address the topic of data protection by design and data protection by default, which are important concepts entailed in the GDPR, through which organizations can foster privacy-conscious culture, and reduce the risk of data breaches thanks to the compliance with the GDPR'S accountability principle, and, consequently, enhancing trust with individuals.

25. *Your right to get your data deleted. (n.d.). ICO. https://ico.org.uk/for-the-public/your-right-to-get-your-data-deleted/#:~:text=The%20right%20to%20get%20your%20data%20deleted%20is%20also%20known,'right%20to%20be%20forgotten'.*

Delving into the specific analysis of this important principle, starting from the concept of Data Protection by Design, it emphasizes the process of integrating data protection considerations at an early stage, into the design and development of systems and processes, encouraging a proactive approach directed to ensure that privacy concerns are anticipated and built into the design, rather than addressing them as an afterthought. As a matter of fact, data protection by design is composed of three key components, which are the conduction of privacy impact assessments (PIAs) which is a process that assists organizations in the identification and management of privacy risks stemming from processes; the implementation of privacy-enhancing technologies; and adherence to privacy principles throughout the development lifecycle. An explicative example of this concept would be the use of pseudonymization to replace personally identifiable material.

On the other hand, relatively to the concept of Data Protection by Default, companies aim to ensure the processing of personal data with the highest level of privacy protection, so that by default data is not accessible to an indefinite number of persons. Under this concept, companies may want, for example, to only process necessary data or for short storage, or limit access to it. In this regard, Social Media platforms should be encouraged to set users' profile settings in the most privacy-friendly manner.[26]

Businesses should in fact comply with these principles to ensure a proper handling of personal data, as well as, as in the case of social media platforms, setting the best way that would allow the protection of the information. As a matter of fact, it is a fundamental responsibility of an organization that is developing in this context to not only comply for themselves but to also ensure that users who may not be fully acculturated on the matter are protected, even when handling situations on their own, for example by limiting the number of accesses per social media platforms' account. Therefore, although organizations that leverage data profiling may gain several important benefits for their businesses, they must take into consideration the serious responsibilities that stem from it, and proactively address them, taking into consideration the data subjects' rights, the required security measures, the existence of a lawful basis for data processing and taking into considerations important provisions such as transparency and accountability, data minimization and purpose limitation.

26. *What does data protection 'by design' and 'by default' mean? (n.d.). European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en*

3.1.2 Economic benefits and associated critical issues from a legal perspective.

Organizations leveraging data monetization benefit from a myriad of economic advantages stemming from different purposes and uses of the latter, whether direct, from increased revenue streams, or indirect with enhanced operational efficiency. Companies that harness the incredibly vast amount of data generated through various sources, can gain significantly valuable insights that range from consumer behaviors, preferences, and market trends, potentially providing competitive advantage.

The insights gained from the collection and processing of data dramatically empower businesses, thanks to their improved capability of making informed decisions concerning various relevant aspects for a successful outcome such as product development, marketing strategies, and resource allocation, which is also directly linked to an efficient steering of the companies' efforts, that can be extremely beneficial as mispositioned resources can be both time and money consuming.

Additionally, the integration of data monetization strategies allows the opening of new revenue streams, such as the sale or licensing of data to third parties and the development of data-driven products and services. Moreover, it is important to consider the fact that data monetization seeks innovation by pushing businesses to invest in advanced analytics, machine learning techniques, and artificial intelligence technologies, to extract valuable insights and use them for business growth. [27]

However, although the incredible economic opportunities presented are comprehensibly appealing, businesses must juggle a complex legal landscape characterized by rigid provisions that entail three main topics: data protection, privacy regulations, ethical considerations, and negligence in addressing them may cost the company severe consequences such as hefty fines or damaging the company's reputation. Among the Legal and regulatory challenges affecting companies willing to conduct data monetization practices, the most prominent ones entail data usage, ownership and liability, and cross-border data flows and global trade.

- Data usage: Companies may stumble across tricky situations due to the limitation of data usage. One of which regards the existence of rules and regulations that prevent them from using their data in any other business venture that differs from the original one, which limits the possibility of data usage and area of action. Similarly, the limitation also concerns the industry in which the business

27. Unlocking financial benefits through data monetization, IBM Blog, February 19 2024.

is operating.[28] As a matter of fact, industries dealing with sensitive information must deal with strict laws regarding data usage, that are imposed to protect individuals' privacy and prevent potential misuse of sensitive information that may concern healthcare and education industries. In addition, to the legal concerns revolving around the topic, it is also important to take into consideration the ethical matter, as the data may derive from industries where data monetization is feasible but is associated with legal dilemmas about selling personal data. Lastly, it is fundamental to mention the importance of considering the lack of control over the use of data once the data is sold, which can lead to the risk of illegal data usage, and potentially managing the reputation of the data provider, who is not responsible for it.[29]

- Ownership and Legal Liability: Data monetization practices pose important situations that must be addressed, one of which concerns the complexity of data ownership due to the non-rivalrous nature of data, which can be used and accessed by multiple parties simultaneously, which can often lead to conflicts over who owns the data, therefore leading to problems over who should be responsible for any negative consequences that may stem from data misuse. As a result, it is fundamental for companies to address liability concerns in advance, where possible, for faulty decision-making or analysis.[30]
- Cross-border data flows and global trade: Data Is transferable; with this premise inputting our analysis, it is important to take into consideration the fact that data that has been collected in one jurisdiction might be transferred to entities that may be located somewhere else, where rules about data processing may be different; which raises significant concerns as there is no coherent and univocal regulatory framework about data sharing and monetization throughout the world. This raises comprehensible questions such as: is the jurisdiction where I am transferring data going to apply the same regulation for privacy protection? Does their system about the topic differ from the jurisdiction of origin of the data? The answers are intricate. As a matter of fact, there are different regulations regarding personal privacy and data handling, depending on the different underlying objectives. While in the EU, there is a single regulatory framework that companies must comply with, the situation is different in the United States, for instance, as there Is no such unified framework, but rather, the jurisdiction differs depending on the state.

28. Parvinen et al., 2020
29. (Tallon, Ramirez and Short, 2013
30. (Thomas and Leiponen, 2016).
31. (Thomas and Leiponen, 2016)

> Given the increasing importance of globalizing data trade, the need for a comprehensive regulatory framework is continuously increasing to facilitate data sharing and monetization while protecting individuals' privacy rights and ensuring data security. Therefore, cooperation may help address these challenges by forming a harmonized regulatory landscape and promoting interoperability in data monetization practices.

In essence, the potential benefits arising from data monetization must be seriously considered, as it affects several aspects that are responsible for the growth of the company and its efficiency, as it can automate time-consuming processes, enhance the customers' experience, and create additional revenue streams. On the other hand, amidst the transformative power of data monetization that companies can harness, it is important to proactively address the challenges it bears, upholding a non-coherent legal landscape, and ethical standards in an increasingly interconnected and globalized market.

3.2 Balancing Profit and Social Responsibility.

Balancing profit derived from data monetization with social responsibility poses an intricate topic that requires a nuanced approach which would entail ethical, societal, and legal compliance implications that temper the mere commitment to economic growth and competitiveness, and foster ethical principles, social values, and the protection of individual's rights.

As a matter of fact, businesses must consider the broader societal impact of their data monetization practice, including addressing potential risks such as discrimination, bias, and exclusion that may stem from decision-making based on algorithms or the use of predictive analysis.

Fairness in data monetization entails ensuring that the propaedeutic actions involved in the process and the derived insights, do not lead to discriminatory and misleading outcomes. As a result, it is fundamental for algorithms to be designed to prevent potential bias, whether based on race, gender, age, or other sensitive characteristics that must be protected. For instance, a company may consider exploiting the collected data, processing it, and monetizing it by developing a personalized pricing practice. This situation provides the proper ground to discuss the cited principle as it must be taken into account by companies when performing such activities to avoid the possibility of putting in place discriminatory pricing models, that may harm vulnerable groups. As a matter of fact, in the article "Big Data's Disparate Impact" by Barocas and Selbst, the authors analyze the phenomenon of discrepancy of treatment that may result from the use of big data analytics, the proper term that should be used to discuss the topic '*is disparate impact'*, which refers to situations where policies

that may seems neutral, actually have a disproportionate effect only on certain demographic groups, leading to uneven outcomes.[32] The authors, in fact, highlight how algorithms trained on historical data may inadvertently encode biases present in that data. To prevent and mitigate such biases, businesses can perform regular audits; including the use of fairness-enhancing tools that can adjust the algorithms toward equal treatment of all groups.

In order to put in place data monetization practices that ensure equal access to benefits and opportunities for everyone, organizations must entail in their practices the principle of equity, which emphasizes the importance of considering in the first place the discriminatory consequences implied in data practices, especially relatively to their impact on marginalized communities. As a matter of fact, while these innovative high-tech tools may promise efficiency and objectivity, they often hide discriminatory outcomes that disproportionately affect vulnerable communities, including indigents, people of color, and people with disabilities. As a matter of fact, it is important to notice how automated systems may not always be the appropriate path to run across, in areas such as welfare, criminal justice, and public services, as it may exacerbate existing disparities and reinforce structural inequality. However, in order to take advantage of this important tool without damaging certain demographic groups, organizations must integrate considerations regarding equity and justice. As to not threaten the human's right to dignity, equal treatment, and inclusivity, avoiding potential stigmatization of individuals and denying access to essential services and opportunities, potentially ''*automating inequality''*. [33] In order to limit the damage of these dangerous outcomes, it is important for companies to ensure that datasets are representative of all segments of the population, and design services that cater to a wide array of needs, facilitating access for disadvantaged or technologically unserved populations.

Lastly, it is vital for organizations that employ data monetization practices, to involve diverse groups in developing data-driven products, services, and decision-making processes. Leading the analysis to the need to understand the last principle necessary for a proper balance of businesses between profits derived from data monetization and societal responsibility: inclusivity. As a matter of fact, it ensures that the benefits derived from big data analytics are shared and widely spread. Not just limited to a privileged subset of the population.

32. Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671-732.
33. Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press

To this end, in her book, “Algorithms of Oppression: How Search Engines Reinforce Racism”, Safiya Umoja Noble explains how search engine algorithms perpetuate racial bias and discrimination, arguing that Google, for instance, often amplifies existing stereotypes, marginalizing minorities by privileging certain forms of knowledge and representation, criticizing the lack of inclusivity and diversity in the algorithms that feed search engines leading to the prioritization of commercial interests and dominant cultural norms, at the expenses of minority communities.[34] An example of this sensitive topic is represented by the bias present in search engines, even in trivial situations such as a person’s interest in searching terms such as ‘black girls’ or ‘Latino immigrants’. The result of the research rarely provides an accurate and diverse representation of the communities of interest, but rather it is much more likely that it will result in deceptive and misleading representations, such as memes, stereotypes, or pornographic content, Influencing the collective ideal of the community.

In essence, embedding societal responsibility in data monetization practices, therefore including principles of fairness, equity, and inclusivity, is essential for long-term business success and social welfare. As a matter of fact, by integrating these concepts into the culture of the organization, businesses can build trust with consumers and local regulations, as well as help the societal acceptance of data-driven innovation, due to the spread of knowledge of the standardized practices that do not just seek profit, without taking into consideration their social responsibility and influence on vulnerable communities.

3.2.1 Legal strategies for a sustainable approach to data monetization, including specific contractual tools.

As evidenced throughout the thesis, businesses involved in data monetization practices must navigate in troubled waters, populated with a myriad of legal and regulatory requirements they must comply with in order to mitigate risks derived from malpractices.

Therefore, to achieve a sustainable approach to data monetization businesses can implement a foundational strategy that involves implementing data governance frameworks encompassing the entire data lifecycle. By doing so companies may easily incorporate privacy-by-design principles, therefore integrating privacy considerations into every stage of the data processing cycle and ensuring proper compliance with regulations such as the General Data Protection Regulation and the California Consumer Privacy Act (CCPA).

34. Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.

Additionally, companies must consider establishing standardized and clear procedures regarding how they will collect, process, and store data to ensure transparency and accountability in their data governance practices, which can be achieved by providing individuals with meaningful choices concerning their data and allowing them to have control over them. Furthermore, a fundamental strategy for a sustainable approach concerns the fact that organizations should maintain records of their data processing activities, to demonstrate, if necessary, their compliance with legal requirements, enhancing their credibility, transparency, and accountability.

Delving into the details of the specific strategies businesses should incorporate, it is fundamental to consider an important tool: Data Processing Agreements (DPAs). A DPA under the General Data Protection Regulation is a contract signed between the data processor that will handle the data and the data controller. It is legally binding as both parties must abide by it or risk severe penalties. Regarding the purpose of the agreement, it establishes the nature, purpose, and duration of the processing activities, and most importantly, it lays out the type of data to be processed alongside the categories of individuals it belongs to and specifies the technical security measures that must be implied such as level of encryption. The main reason for the existence of such a contract lies in the fact that it ensures the qualification and accountability of the data processor, allowing companies to have the assurance they need to know their data is safeguarded.[35]

Additionally, businesses engaging in data-sharing arrangements with external organizations may consider implementing data-sharing agreements to regulate the exchange of data between the involved parties and contribute to compliance with the accountability principle. A DSA establishes the terms and conditions under which data can be shared. It includes the rights of each party, the obligations they must comply with, the purpose for which the shared data will be used, and the limitations regarding the disclosure of the content and the security measures implied. As a matter of fact, the purpose of such a tool is fundamental as it allows to explain the specific aims of the data-sharing activities the parties are willing to take part in, the reason why such activity is crucial to the achievement of such aims, and the benefits expected for individuals or society[35]. Data Sharing Agreements play a crucial role in facilitating responsible data-sharing practices, increasing the parties' credibility and accountability as it ensures compliance with legal requirements.

35. ICO. (n.d.). *Data sharing agreements*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/

To achieve the ambitious goal of sustainable data monetization practices organizations can implement systematic processes that facilitate the assessment of potential privacy risks associated with a specific data processing activity or project: Privacy Impact Assessment (PIA). The instrument was introduced with the General Data Protection Regulation (Art. 35 of the GDPR), and it must always be conducted when the processing may conclude in a high risk of damaging a natural person's rights and freedom, which includes profiling automated practices that may lead to legal consequences for the people involved, processing of data about incapacitated persons or those with limited ability to act, data transfer to countries outside the EU/EEC, and the merging of data which was gathered by various processes. [36] By assessing the potential risks derived from the processing of certain categories of data, this tool can help organizations understand how their data activities may affect privacy rights, whether any privacy risk needs to be mitigated, and it typically covers the project or system entirely ensuring safety through the entire data processing activity.

Subsequently the assessment of privacy risks is the additional step that concerns the evaluation of data processing compliance with the relevant laws, industry standards such as the GDPR, or specific sectoral regulations. Finally, after implementing the required strategies for risk mitigations that may have emerged from the assessment, organizations should document the findings of the PIA and report it to stakeholders or regulatory authorities, as required.

Such practice would not only allow proper risk identification and mitigation, as well as ensure compliance with legal requirements, but also stakeholders' confidence. As a matter of fact, being accountable and transparent regarding the security of the processing enhances trust and confidence among customers, stakeholders, and authorities.

Thanks to the implementation of such legal tools, along with strategies that incorporate awareness programs for employees involved in data handling activities, and purpose limitations, companies can ensure compliance with data protection laws, mitigating reputational risks derived from data storage, sharing, and processing, therefore demonstrating their proactive willingness to adhere to principles of accountability, transparency, and ethical responsibility.

36. *Privacy Impact Assessment - General Data Protection Regulation (GDPR)*. (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/privacy-impact-assessment/

Chapter 4: Case Study – Facebook

4.1 Facebook Company Profile.

It is evident how some companies' actions can affect certain sectors differently from others, depending on their influence, the vastity of the population they manage to reach, and the force of the consequences of illicit actions on the stakeholders. In this concern, Facebook, now rebranded as Meta Platforms, Inc., carries the responsibility of such relevance and influence on the sector they operate in.

Facebook is a social media platform and social networking service, created in 2004 by Mark Zuckerberg and some of his college colleagues. As a matter of fact, the subscription was initially limited to Harvard students as a networking system, which then expanded to other Ivy League colleges. Two years later membership was permitted to everyone who met the required age of thirteen years old. Fast forward to 2010, Facebook was the most downloaded mobile app, and in 2023, it ranked third as the most visited website in the world, thus confirming its relevance in the sector and, therefore its importance in complying with regulations.[37]

Regarding the platform's main revenue stream, the company's business model majorly relies on advertisements, as a matter of fact, due to the absence of subscription fees required, in 2020, of the total revenue, approximately 97.9% derived from it.[37] In this regard, Facebook managed to offer advertisers the ability to target the desired demographics, based on age, gender, location, language, and most frequently clicked topics. Additionally, advertisers can track the performance of the placed ads through standardized metrics provided by the platform, increasing their visibility, building brand awareness, and helping define the goal of the promotion.

To this concern, it is evident how profiling assumes a pivotal role in shaping Facebook's business model as it heavily relies on targeted advertising to allow marketers to reach the desired audience, therefore gaining the best benefits that can be earned from such activity. As a matter of fact, the platform collects a vastity of data from its users, intending to offer advertisers the best service,

37. https://en.wikipedia.org/wiki/Facebook
38. https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/#:~:text=In%202020%2C%20about%2097.9%20percent,increase%20in%20comparison%20to%20the

this includes the ability to deliver personalized ads to those who would most like to engage with them.

The Sophisticated activity of data profiling involves the collection of personal information, including name, age, gender, location, and phone number, which helps identify the person in the process of account creation, as well as behavioral data that concern the interaction of the user with various elements of the platform, such as the comments it leaves under the posts presented, likes, and more specific information like the amount of time spent on specific advertisements and posts, in order to identify, one hand, a particular attitude and general preference of the user, therefore enhancing the customer's experience, allowing the creation of a customized app by mainly suggesting content preferred by the customer, on the other hand, provide marketers additional important information that allows specific targeting of the desired customer segment.

In this concern, it is important to cite Facebook Pixel, now Meta Pixel, a piece of code placed on the website that helps track users navigating the website by collecting data to optimize targeted advertising and analytics. This useful tool, created by Meta Platforms Inc., allows businesses to collect data from their websites which can then be used to improve the effectiveness of the advertisements that will consequently run on social media platforms such as Facebook and Instagram, helping businesses to have a broader and deeper understanding of their audience and the performance of their campaigns.

The data collected from the pixel is sent to Facebook's servers which will utilize it for the primary purpose aforementioned, as well as for its ad delivery algorithms to enhance the users' experience by showing content they may find to be more relevant and ensuring that users are targeted with ads based on their online behavior.[39]

To better understand the functioning of this tool, therefore capturing its relevance to the analysis conducted in this thesis, it is fundamental to understand the foundational topic that serves as a base for this concept: "retargeting"; thanks to this, companies, can make the best of the data used from Facebook Pixel to show their ads to users who have at least once visited their website. In fact, this form of online advertising's purpose is to re-engage users who have interacted with a certain brand

39. https://blog.hootsuite.com/facebook-pixel/#:~:text=The%20Facebook%20pixel%20is%20a%20piece%20of%20code%20that%20you,of%20action%20on%20your%20website.

but did not complete the expected action, such as purchasing or filling out a required form, and can potentially lead to several benefits, such as increased conversion, as it helps retarget users who have already shown interest in the content. Furthermore, it leads to more cost-effective strategies as it focuses on users who are already familiar with the brand and have already shown interest, and therefore may be keener to fulfill the desired action, without requiring large budgets that would be needed to acquire an audience whose interests are unknown.

Regarding the implications for users apart from the ones related to the creation of detailed profiles aimed at delivering highly targeted advertising, it is fundamental to address the concerns related to privacy. As a matter of fact, Facebook Pixel collects data from website visits and integrates them with a much broader data ecosystem. Because of the possibility that users may be unaware of such practices, it is vital for Facebook Pixel to inform users through clear and transparent information regarding the use and sharing of their data, as well as the fundamental opt-out mechanisms they can use to be excluded from such practices because of the real chance for users to feel uncomfortable with the fact of being followed by advertisements related to their internet browsing history. Additionally, users must be protected from unauthorized access and disclosure therefore they must be granted secure data storage and protection of their personal information, as a matter of fact, websites using Facebook Pixel must comply with transparency requirements entailed in the GDPR and the CCPA.[40]

As a matter of fact, Facebook Pixel is an incredibly useful tool that companies can make the best of by allowing targeted advertising and the segmentation of communities of users related by their interests. Although the numerous benefits it offers, the evident concerns related to privacy must be taken into consideration and addressed, as a matter of fact, the tool presented serves as an example in the attempt to demonstrate how integrated data profiling practices are in Facebook's business model, which implies the implementation of transparency strategies and the data security to avoid possible limitation of freedom of the users and their fundamental right to privacy.

Therefore it is fundamental for companies, including influential ones such as Facebook, to comply with the requirements of the GDPR provisions which include explicit consent from the users whose data is being collected and processed, the obligation of transparency toward customers about the activities related to their data, and the right for the data subjects to access their data anytime, ask for corrections, and deletion under proper circumstances.

40. https://sproutsocial.com/glossary/retargeting/#:~:text=Retargeting%2C%20also%20called%20remarketing%2C%20is,displaying%20ads%20or%20sending%20emails.

In this concern, it is fundamental to introduce the infamous Cambridge Analytica Scandal that took place in 2018 as an example. In fact, it revealed the unauthorized access to data of millions of users without their consent, leading to the company's non-compliance with the provisions entailed in the regulatory landscape, and to a mediatic echo that caused many users to be more aware of their rights, confirming the importance of compliance with rules and regulations. As a matter of fact, the problematic scenario and the numerous outcomes derived from it will be later discussed in detail due to their regulatory relevance, mediatic impact, and the outcomes derived. [41]

In conclusion, Facebook's use of data profiling to improve its main source of revenue assumes a leadership role in dragging digital advertising practices and strategies and poses significant challenges both from a legal and ethical perspective that the company must continuously update and address to maintain compliance and protect users' privacy.

4.2 Facebook Profiling Practices

As mentioned in the previous section of the thesis, Facebook's business model deeply relies on advertisements as its main revenue stream. The company manages to be so efficient mainly thanks to the profiling practices of their users, which allow the collection of a vast assortment of data which is then analyzed, allowing the creation of a user's profile.

The specific aim of such activities differs from mere monitoring but rather aims at providing advertisers with exact and meaningful information that allows precise targeting of the desired demographics and interests, leading to an unmatched degree of efficiency for an activity that would be both time and money-consuming.

However, despite the proven and evident results and benefits that both the company and marketers can gain, the profiling practices that allow the activation of these intricate mechanisms have raised relevant legal and ethical concerns, concerning matters of adherence to regulatory frameworks, consent from users regarding the use of their personal information, and aspects such as the right to be informed and right to personal privacy; which are particularly given evidence by the Cambridge Analytica scandal, due to its involvement with psychological profiling of users conducted to create personalized advertisements that have significantly impacted political campaigns such as the United States Presidential election in 2016 and the Brexit Referendum, and most importantly, the profiling activities took place without explicit and informed consent from data subjects and equal importance

41. https://www.dirittoconsenso.it/2021/12/21/il-caso-cambridge-analytica

must be provided to the ethical implications stemming from data-driven political influence,[42] of which will be largely given space in the following section.

Following the provisions in the General Data Protection Regulation, any personal data of European Union citizens collected and processed by organizations must be conducted on a legal basis that allows the processing. In this concern, Facebook asserts the existence of several legal bases for its data processing activities. Specifically, three main foundational grounds are identified:

- Consent: Facebook relies on user consent to process data through several methods, such as User Agreements and privacy policy, of which terms the user agrees to when signing up in the platform; Notification of Changes to its data practices or privacy policies, and users are given notice of the presence of Cookies and tracking technologies when they visit the website, as well as opt-out options. [43]

  However, there have been concerns about the validity of the consents obtained from the users, which mainly regard the complexity and the length of the terms and privacy policies which are overly difficult for the average user to understand or read thoroughly. Additionally, consent is often bundled with the acceptance of general terms of services, making the distinction between different data collection and processing activities. Finally, the most relevant aspects concerns the insufficiency of transparency as user may not be totally aware of the vastity of the data that is being collected, which data, how it will be processed, and with whom it will be shared, leading to the problematic situation presented by the Cambridge Analytica Scandal, that evidenced how users had no idea of the extent of the data sharing activities that were taking place.[44]

  In addition to that, some regulators in Europe have contended that Facebook does not obtain users consent lawfully as it was not explicit nor informed regarding the tracking and data collection from other sites and apps. The general concern regards the fact that a large section of the 2.1 Billion users actually do noy know the vastity of the amount of the data that Facebook can collect, and how it can use it. This concept leads to a general concern and

42. https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/
43. Facebook's Terms of Service and Privacy Policy: https://www.facebook.com/legal/terms/?paipv=0&eav=AfYcGnmXmKW18lUcoezaUtpQOSfH4Y7c_87ZwMoBxns6dFgIf_s25CYwgYnWeHLo25A&_rdr
44. Academic Analysis: Barocas, S., & Selbst, A. D. (2016). "Big Data's Disparate Impact." *California Law Review, 104*(3), 671-732.

A growing feeling of discomfort relatively to the unfair ability of tech giants to manipulate users.[45]

- Contractual Necessity: Facebook argues the existence of an important lawful basis for its data processing activities which is the need for such activities to take place as it is necessary for the fulfillment of the contract between the company and its users.
- Legitimate Interest: The company claims that they have consistent and reasonable purposes to conduct the profiling practices as they are also imputed to the need and desire of improving the services provided and enhance security posture of the platform, therefore detaching themselves from mere profit interests. However, it is important to consider that this basis requires careful assessments as it must be rightfully balanced as to not harm the rights and freedom of the data subjects.[46]

Moreover, it is fundamental to take into consideration the meaning of profiling, which is referred to, under the GDPR, ad any form of Automated Processing of personal data to analyze and evaluate specific aspects concerning the individual's private sphere: performance at work, economic and financial situation, health, reliability, and location.

In this regard, the GDPR requires companies to clearly inform the data subjects about the data that is being collected and the purpose for which it will be used. Relatively to Facebook, the critiques in this concern are numerous as the opacity of the data collection practices and the lack of clarity of the privacy policies do not allow users to be informed about the use of their sensitive information.

In addition to that, Facebook has faced legal challenges concerning its compliance with the safeguarding of the data subjects' rights. Specifically, regarding the rights to access their data in any moment and the processing of the latter as well as the categories of data that are being processed; secondly, the right to have, if present, inaccuracies rectified, therefore allowing the correction of inaccurate or outdated information promptly; thirdly the right to have their data erased, which is included in the right to be forgotten and applies in cases in which data is no longer necessary for the purpose for which it was collected or, for example, unlawful processing of data. The last right mentioned poses a significantly problematic situation as ensuring complete deletion of the

45. https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html#:~:text=But%20in%20Europe%2C%20some%20regulators,the%20company%20could%20use%20it.
46. ttps://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0

information collected can be particularly insidious in such a complex network, that involves different actors, forming a complex landscape in the desire of granting full erasure from the systems. As a matter of fact, there have been numerous cases in which users have requested the deletion of their data, but still managed, after time, to find traces.[47]

What must be take into consideration as particularly uncanny of the rights that the company still has difficulties to grant is the fact that technological giants actually manage to manipulate users not only with the intricacies of their terms of use, policies, and privacy practices, but also through the fact that because of their complex systems they cannot grant rectification because of the complexity if their data infrastructure and volume of the data stored, and cannot grant full erasure because of the fact that the data collected from the company actually navigates across a vastity of integrated third-parties.

In conclusion, the legal analysis of Facebook's profiling practices, reveals significant absences in different yet fundamental topics, such as transparency, consent, and data security, which highlights the stringent need for strict regulatory frameworks that also oblige compliance for giants of the sector, to protect users' privacy and rights, allowing ethical data handling practices. As a matter of fact, it is fundamental for businesses to strike a balance between their need for innovation and profit-related interests, as well as building trust within costumer thanks to compliance with legal standards and ethical practices.

4.3 Ethical and Privacy Implications in the Facebook Case.

The specific case that will be analyzed in this thesis to exemplify the concepts outlined throughout the text, analyze the legal and ethical concerns that until this point have been examined theoretically, and lastly study the outcomes derived is the Cambridge Analytica Scandal, as it provides proper space to highlight the vulnerabilities in digital data practices and the potential misuse in specifically dangerous contexts.

As a matter of fact, after providing enough information about Facebook's profiling practices and the regulatory frameworks it must comply to, it is fundamental to delve into the details one of the most intricate cases that involved the company. Analyzing the ethical and legal implications that directly concerned Facebook as it played a central role in the matter and third parties.

47. https://www.apiscene.io/api-security-identity/data-deletion-at-facebook/

The two main characters in the situation were Cambridge Analytica and Facebook.

The first one was a British political consulting firm that main specialized its activities in data mining, analysis, and strategic communications, and claimed to use the outcomes derived from data to create precise psychological profiles of voter to influence their behavior in advantage of whoever they desired.[48]

Facebook, on the other hand, plays a crucial role in the situation as it allowed external apps to gather data from not only users who have installed them, but also from their friends, often without explicit consent, which traces back to the absence of explicit consents and transparency on the matter from the company.[49]

The scandal started with an app called “This Is Your Digital Life", founded by a researcher at Cambridge University called Aleksandr Kogan. The app, as It was presented as a personality quiz had been downloaded from approximately 270’000 Facebook users. However, due to the fallacies in the Facebook’s policies, the app actually harvested data from around 90 million users.

The founder of the app, against Facebook’s policies, decided to sell the data, which included personal information such as likes, friends, and other profile details that concerned the personal sphere of the user to Cambridge Analytica which that intended to use them to build voter profiles.

The harvested data was later utilized by Cambridge Analytica to build predictive models with the aim of influencing voter behavior, leading to not only important legal concerns due to the practices that took place until this moment, but also on the ethical sphere as it questions the unconscious influence that users of social media and various websites undergo without them even noticing it. This malpractice involved two main streams: Micro-targeting and behavioral influence.

The first one entailed tailored political advertisement directed to individuals based on the psychological profile that has been identified, and their preferences. The micro-targeting led to hyper-specific advertisements that addressed people’s fears and concerns relatively to important political topics. For example, the ads placed might have emphasized the danger of immigration and

48. https://en.wikipedia.org/wiki/Cambridge_Analytica#:~:text=Cambridge%20Analytica%20was%20established%20as,royalty%2C%20and%20the%20British%20military.
49. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
50. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

loss of national sovereignty concerning the Brexit referendum, while enhancing the economic opportunities that could have been gained outside the European Union to those whose concerns were directed to economic issues.

Behavioral influence, on the other hand, involves the use of psychological hints to emotionally trigger viewers that see the advertisements with the aim of unconsciously shift perceptions and motivation.

An additional example of the influence that such case has brought to the political landscape, it is useful to introduce the role that Cambridge Analytica has played in the Trump campaign. As shown in the figure below, selected as representative of the strict interplay between the actors. In fact, it is shown in the diagram the involvement of Alexander Nix, the CEO at the time of the events, Steve Bannon, Vice president of Cambridge Analytica who later has become chief strategist for Donald Trump, and Robert Mercer, a wealthy, majorly conservative, that decided to fund the political consulting firm. [51]

The firm's ability to harvest vast amount of personal data and its ability to create precise psychological profiles and targeted advertising had a major impact also on the 2016 United States presidential election. As a matter of fact, the company has closely worked with the Trump campaign to micro-target voters with emotionally charged ads, to influence voters and swing the

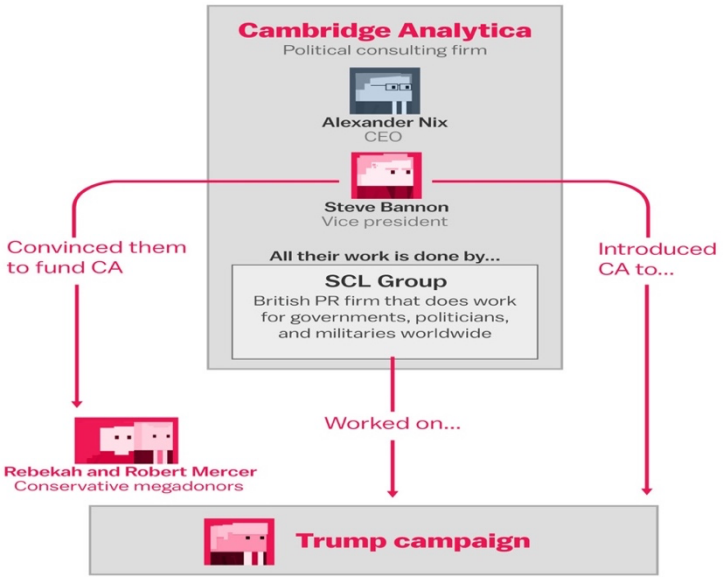

Figura 1[52]

51. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
52. https://www.informationisbeautifulawards.com/showcase/3673-the-facebook-and-cambridge-analytica-scandal-explained-with-a-simple-diagram

election in Trump's favor.[53] The practices led to three main consequences that concerned ethical questioning, Privacy violation, regulatory scrutiny (Facebook has in fact faced severe fines for its role in allowing data breach), and political influence.

Relatively to the ethical concerns, it is fundamental to firstly take into consideration the manipulation of the users that took place in the scandal. As a matter of fact, such molding of the individual's voting preference using data for psychological profiling and targeted political advertisements, raises relevant critiques about the individual's autonomy due to the influence the users were subjected without them knowing, and importantly, without their explicit consent, potentially damaging the democratic principles. From the legal point of view, it is fundamental to take into consideration the fact, that manipulation violates the Article 5 of the GDPR, which specifically requires transparency and fairness in data profiling practices, provisioning that user's rights to be informed about how their data is used and to consents, both of which have been violated.[54]

Secondly, concerning the ethical aspects that impacted the situation, it is fundamental to consider the fact that trust is a fundamental aspect for companies, especially for those known to be handling personal data. In fact, users were oblivious about how their data was being collected and used for purposes that have not been declared, in this case, political goals. The lack of transparency concerning the use of the data is particularly problematic, not only from the ethical perspective, but also from a legal point of view, as it is specifically outlined in the GDPR, specifically in articles 12-14, that Data controllers are required to provide data subjects with clear, easily accessible and to understand information about the data processing activities, and in this concern Facebook significantly lacked in the ability to fulfil such requirements.[55]

Finally, the scandal also has the merit of providing evidence of the already existing issues concerning equity and fairness, that as already evidenced several times throughout the thesis is a fundamental principle that must characterized all companies willing to continue their profiling activities in a sustainable manner. As a matter of fact, the use of the harvested data to micro-target very specific demographic groups, particularly easy to manipulate, is an evident manner of exploiting certain people's vulnerabilities, leveraging on their fears and dreams to maneuver the

53. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
54. https://gdpr-info.eu/art-5-gdpr/
55. https://gdpr-info.eu/art-12-gdpr/

political landscape. The concerning problematic of the matter are particularly evidenced from the fact that the GDPR in art. 5, specifically emphasizes the importance of fairness in data processing, therefore meaning that data should not be used in ways that harm certain groups disproportionally.[56]

Apart from the ethical concerns, that evidently deserve their fair share of space in the discussion of the matter, it is also important to consider the privacy issues related to it.

The first privacy issue concerns the absence of informed consent. As a matter of fact, providing genuine consent ensures that the data subject is fully aware that its data is being collected, and that the company is totally sure of the user's agreement. Unfortunately, this fundamental aspect missed, leading therefore to a violation of privacy rights, as it is actually required by art. 7 in the GDPR specific, informed, and freely given consent.[57] However, as previously outlined, Facebook's policies on consent mechanisms undermine this principle mainly due to its complex architectural nature.

Moreover, the scandal shed light on the severe scarcity of the company concerning data security posture, which in fact, allowed third-party entities to access incredibly vast amounts of data from their users, not just from the one who actually downloaded the app, but also those who were in the network of the downloaders, without sufficient control. The oversight of the security of the data of the users would in fact be Facebook's responsibility, to which it did not live up to. As a matter of fact, art. 32 of the GDPR provisions that companies must comply with appropriate methods, both from a technical and an organizational point of view, to grant users the best security that can safeguard their data.[58]

Finally, Facebook did not manage in this situation to comply with GDPR Articles 5(1)(c) and 5(1)(b), which require that personal data must be retained for what is necessary, it must be relevant for the purpose, and adequate, additionally, it must be collected for specified, explicit, and legitimate purposes.[59] As a matter of fact, it is evident how the company collected data extensively, pushing its practices far beyond the claimed goals, providing evidence of how they were not justified for activities they claimed to be necessary to provide the services and fulfill contractual agreements with the user.

56. https://gdpr-info.eu/art-5-gdpr/
57. https://gdpr-info.eu/art-7-gdpr/
58. https://gdpr-text.com/read/article-32/
59. https://gdpr-info.eu/art-5-gdpr/

The scandal was brought to light by a former employee of Cambridge Analytica, Christopher Wylie, who subsequently testified before UK parliamentarians, and gained an incredibly extensive mediatic resonance after being reported by The Guardian and the New York Times in March 2018, revealing the violation of around 50 millions of Facebook Profiles.

The reported timeline of the scandal shows the stringent sequence of events that followed the news leak, which in the meantime implied extensive mediatic coverage leading to significant public outrage, universal scrutiny of Facebook's activities related to data and investigations.

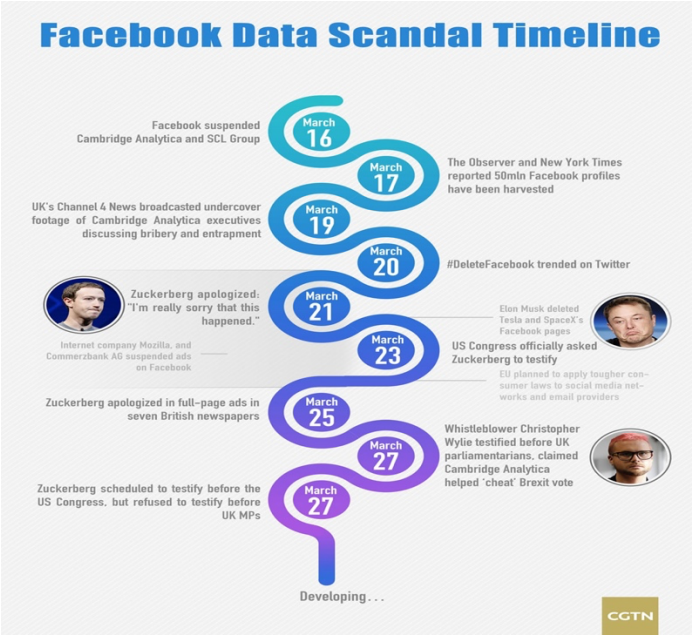

Figura 2[60]

In this scenario, it is fundamental to analyze Facebook's responses as particularly interesting since they covered diverse aspects that have been impacted, all relevant to rebuilding trust with the consumer and the regulators.

Firstly, Facebook updated its privacy policies to enhance transparency and provide users with detailed information about how their data is used,[61] therefore addressing the fundamental matter of transparency and informed consent demanded in Art. 12-14 of the GDPR, which have, until now, been overlooked.[62]

60. https://news.cgtn.com/news/3063544f306b7a6333566d54/share_p.html
61. Facebook Data Policy Facebook Data Policy https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0
62. https://gdpr-info.eu/art-12-gdpr/

Secondly, the company ensured to strengthen Consent Mechanisms entailed in their platform, guaranteeing that users are aware of what they are agreeing to,[63] demonstrating that they are informed of the terms entailed about the data collection activities and usage to align with the high standards required from the GDPR, particularly in article 7, In which it Is specified the need for the company to only use the data collected for the purposes that the data subject agreed to at the time of the agreement, matching the need for explicit and informed consent.

Additionally, Facebook established a Privacy Committee to oversight privacy mechanisms and the overall security posture to enhance credibility and accountability of the data handling activities, hopefully restoring the damaged public vision. In this concern, the company addressed the fundamental matter of accountability in data processing required in articles 5 and 24 of the GDPR.[65]

Lastly, the company committed to working closely with regulatory authorities to address data protection concerns and ensure compliance with legal requirements. 66 The commitment toward the desire to address the deficiencies of the company in complying with certain fundamental requirements of the GDPR can be seen as a will of transparency and an additional step in the attempt to repair the damages of the past, that have significantly shaken users and their trust in the organization.

Following the incident, Facebook faced multiple legal and regulatory challenges, which included a 5 billion dollar fine by the Federal Trade Commission (FTC) for privacy violations, investigations conducted by the Irish Data Protection Commission, and broader consequences for companies working in the tech industry that imply stricter regulations on data privacy and increased scrutiny on data processing activities.[67]

63. Facebook Data Policy Facebook Data Policy https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0
64. https://www.altalex.com/documents/news/2018/04/12/articolo-7-gdpr-condizioni-per-il-consenso
65. https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/
66. https://www.edpb.europa.eu/edpb_en
67. *Reference: Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671-732.*

As identified throughout this section, it was evident how there have been several responsible actors in the scandal, who all played a significant role in the extensive data collection practices, in the failure to comply with the GDPR and obtain genuine and informed consent, in the manipulation of voter behavior and erosion of autonomy through the use of micro-targeting activities and inadequate data security practices. This case has, in fact, provided a proper space for reasoning for the massive influence of technological giants in our everyday life, in their ability to unconsciously condition individual's choices and potentially harm genuine freedom of choice, and most importantly, their responsibility in avoiding malpractices at all costs, because of the impact on users, and because of their impact on less influential organizations.

4.4 Conclusions from the Facebook Case

The Facebook-Cambridge Analytica scandal has highlighted the need for important attention toward robust data protection and privacy measures, to safeguard individual's personal autonomy ensuring that they have full control over their personal information, allowing them to make informed decisions, and to be aware of the purpose of the data collection activities, genuinely granting access to their data thanks to the clear information they have been provided with. In addition, the misuse of data processing activities, therefore of the data subject's personal information, is one of the main reasons that lead users to lose trust in the company, mainly due to the fear of unethical profiling activities.

As a matter of fact, the malpractices highlighted in the scandal evidenced the existing vulnerabilities in complex systems and highlighted the need for more stringent data governance practices. The incident firmly impacted legal frameworks, as it accelerated the implementation and enforcement of comprehensive data protection laws such as the General Data Protection Regulation in the European Union to improve topics that have been overseen, such as the importance of informed consent, the need for data minimization, which refers to the principle of collecting only data that is necessary for the declared purposes and the fulfillment of the services that the users expect.

Additionally, the scandal has put the accent on equally important themes such as transparency and accountability in data collection practices. As a matter of fact, it is fundamental for companies to be transparent about the categories of data that will be collected, the correlated activities that will be conducted, and who it will be shared with, contrarily to what Facebook has provided until this

moment to its users, allowing important data breaches and external parties to have access to both the data of the people who took part on the quiz and of those who were part of their network.

Companies are now expected to be more accountable from this point of view, and they must ensure their compliance with legal standards and take into serious consideration ethical concerns, which includes the conduction of regular audits, transparency about the data usage policies by also making them easily readable and understandable from the average user, and being prepared to take responsibility for possible data breaches. [68]

As a matter of fact, although the intrinsic intricacies of such a complex system as Facebook can be, it is fundamental for influential and enormous companies to recognize the responsibilities that derive from the interaction with so many users, many of which may also be inflicted with disproportionately affected as part of vulnerable communities.

An additional fundamental lesson learned from the scandal lies in the importance of user empowerment. This concept underlines the necessity to provide users with the ability to have control over their personal data as it represents an essential matter for individual affirmation and freedom of choice. In practice, it includes providing easily understandable privacy settings, clear consent mechanisms, and the ability to opt out of data-sharing agreements.

In this concern, the General Data Protection Regulation provisions that companies must ensure users have control over their data. In particular, they must be priorly informed of their rights which include the possibility of accessing their data at any moment, the right to correct mistakes in the present data, under certain circumstances, deletion, and the right to data portability.[69]

The scandal's incredible resonance is highlighted by the fact that it initiated broader implications for the digital world, in particular, it impacted three main aspects: improved regulatory oversight, Technological and Ethical considerations, and Market and Consumer Trust.

Specifically, the Cambridge Analytica scandal initiated increased regulatory oversight over the data practices of tech companies worldwide, setting a precedent for which Government and regulatory

68. Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.
69. European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Organizations are now more attentive and proactive in monitoring and preventing how companies handle user data.

As a matter of fact, it must be taken into consideration that the companies involved in such malpractices may be doing so because they might gain even a larger profit as in the case of Cambridge Analytica in which several actors with different aims have been involved, and although the hefty fines and severe consequences they had to face, it may probably be asserted that it would be too late as some of their goals have already been accomplished throughout the process. Therefore, it is fundamental for regulatory bodies to have control over such organizations and even prevent their possible desire to conduct unethical data processing activities.

In fact, as a result the incident had a global impact that also affected countries outside the European union to reconsider their own data protection laws, as to not trip over possible data breaches, that may harm users and potentially also their reputation and credibility. For instance, the California Consumer Privacy Act in the United States was strongly influenced by the provisions of the GDPR, and the Cambridge Analytica scandal accelerated the demand for more robust data privacy laws in the U.S.[70]

Secondly, the case managed to highlight the need to take into serious consideration the ethical concerns related to the development and deployment of technology. As a matter of fact, data processing activities are a particularly useful and meaningful tool, that can help organizations improve the user's experience, and provide the best service including the ability to mostly show what the consumers are interested in, however, the ethical concerns must be addressed, especially when automated data processing activities and artificial intelligence are implied due to their unfortunate ability to threaten democracy, as seen in this specific incident, and increasing inequalities.[71]

In this concern, companies may consider establishing best practices for ethical behavior concerning data, including the principles of fairness, transparency, and accountability, as they have become crucial for a sustainable approach to innovation. These ethical principles may be initiated by adopting privacy by design and privacy by default principles in the technological system as to ensure the best approach from the foundations.

70. California Legislative Information. (2018). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa
71. O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Broadway Books.

Lastly, it is fundamental to take into account a matter of fundamental interest for companies: market and consumer trust. Building and maintaining consumer trust requires continuous and consistent efforts relatively to several aspects such as transparency, ethical data practices, and responsiveness to user concerns. Companies that show a genuine commitment to such practices are more likely to build customers' trust and loyalty, therefore, retaining their audience.

On the other hand, companies like Facebook that fail in this aim, face significant reputational damage that may lead to long-term financial damages.

In this concern, the bar chart below, which represents the result of a survey conducted on 1012 people who have ever had a Facebook account, has been reported to support the proposed thesis. As a matter of fact, the graph analyzes the reasons why people have deleted their Facebook account, and the data shows that:

- Around 66% of people who have completely removed Facebook from their lives do not want the social media platform to have their personal data.
- Around 61% were worried about their privacy.

As a matter of fact, 2018 was the year that witnessed the Cambridge Analytica scandal, the polemics that derived from it, as well as the ethical and privacy protection concerns.

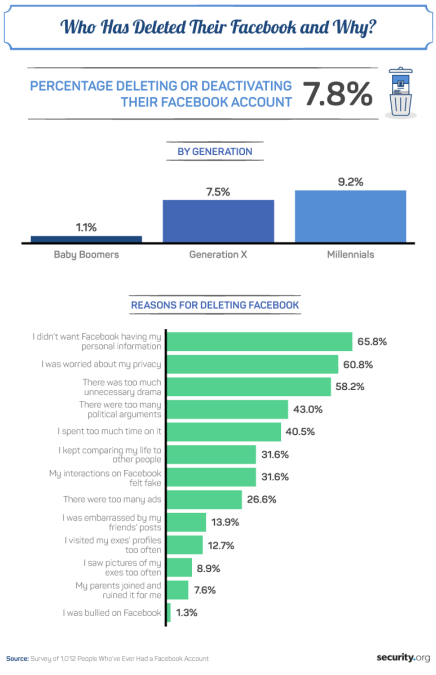

Fig. 3[72]

72. https://www.security.org/resources/detailing-delete-facebook-phenomenon/

Although it is not possible to determine with absolute certainty the correlation between the deletion of the accounts and the scandal, it is reasonable to believe that there is some kind of link between the two events. As a matter of fact, it is evident from the reasons for the deletion of the accounts that Facebook's inability to protect its users, and the lack of commitment to legal provisions have seriously impacted users and their trust in the organizations. Potentially making them more aware of the real practices conducted on their personal information, and the real hidden interplays they were unaware of.

The presented bar chart is only a relatively small representation of the damages of malpractices and their impact on user's trust in the organizations, especially when their data is being collected for automated processing activities that may be potentially harmful and dangerous both for certain vulnerable demographic groups and the society as a collectivity, highlighting once again the relevance of approaching data processing activities lawfully, ethically, and transparently.

4.5 Summary of Key Findings.

The research conducted throughout this thesis has revealed interesting insights regarding data profiling activities, privacy regulations, and ethical implications. Firstly, starting from a more theoretical perspective to provide the proper terminology, adequate information on the regulatory frameworks that concern the discussed topic, and a detailed explanation of the importance of data profiling activities, and the economic and organizational benefits derived from it.

The second part of the thesis delved instead into a glaring case study that involved Facebook, also known as the Cambridge Analytica scandal, since it provides the proper ground for ethical and legal considerations, as well as gives evidence of the actual impact of technological giants on different aspects, for instance, indirect manipulation of political campaigns, and their ability to influence users freedom of choice thanks to the capacity of profiling psychological aspects. In addition to that, the case study evidences the importance of complying with regulatory provisions and building trust within customers. Most importantly, the scandal that derived from the situation created an echo that resonated and impacted several organizations in the Tech Industry across the world, leading to a global impact.

More specifically, throughout the thesis, it has been evidenced numerous times the importance of Data Privacy regulations. As a matter of fact, the General Data Protection Regulation has had an

incredibly impactful influence on setting the global standard concerning individual privacy and data protection, with a strong emphasis on the necessity of obtaining informed consent that must be freely given and as a result of a conscious choice, evidencing, once again the importance given to freedom of choice and consent to the treatment of personal data. Additionally, it has been highlighted in the research the importance of data minimization, as to reduce the time of data retention, and the purposes. Finally, it has been given particular importance to the implementation of robust security measures to avoid data breaches that may grant access to personal information to processors with malicious intentions.

Moreover, a fundamental topic concerns the need for data profiling practices to be transparent. As a matter of fact, most of the legal issues concerning data profiling malpractices are attributed to inadequate user consent that may be due to complexity and opacity in privacy policies that are submitted to users, as a result, users do not provide their genuine and informed consent.

Despite companies' desire to claim the presence of legitimate interests and contractual necessity as a legal base for data processing most of the time, regulatory bodies like the Federal Trade Commission have often found that there has been in reality a violation of privacy standards.

Lastly, the ethical implications concerning the data profiling activities, and in particular the scandal analyzed in the second part of the thesis, underscore the importance of transparency in data processing activities, as they may be exploited for purposes that do not aim at enhancing the services provided, but rather for political manipulation or profit, leading to broader discussion on the ethical responsibilities of data controllers and processors, and the need to set proactive measures and best practices to prevent unwanted situations.

To summon the importance of what has been just mentioned, I will introduce a particularly relevant citation extracted from "A predictive privacy impact assessment: The case of Profiling." Computer Law & Security Review, 35(1), 105324, that I have found to be particularly meaningful and impactful.

"Profiling, when conducted unethically or unlawfully, can result in significant harm to individuals, including discrimination, loss of privacy, and erosion of trust in digital systems. To prevent these negative outcomes, it is imperative that profiling activities are performed with strict adherence to ethical principles and legal frameworks. This includes ensuring transparency, obtaining informed

consent, safeguarding against biases, and providing individuals with the ability to access, correct, and challenge the data and decisions that affect them. By upholding these standards, organizations can protect individual rights and maintain public trust."[73]

As a matter of fact, the citation manages to summarize the critical importance of the need for ethical and lawful practices in profiling to prevent harm and protect individual's rights.

In this concern, it is fundamental to provide a comprehensive analysis of the topic to provide insights into the lessons learned and my personal findings, specifically focusing on future steps that may be implied.

Throughout the thesis, it is evident that a constant topic that reoccurs as central to the matter is the need for implementing robust legal frameworks to govern data privacy and protect consumers' personal information. In this concern, effective enforcement of data protection laws is crucial in holding companies accountable and ensuring compliance.

Therefore, it is fundamental for companies to strike a balance between the need to keep up with the fast pace of innovation, leveraging data for profits, and ensuring the protection of users. As a matter of fact, tech giants must take into consideration their ability to model people's lives through their content, because of the strict existing bond of the average person with technological devices and social media platforms. The collection and analysis of data can in fact boost the companies' profitability and efficiency, enhancing their ability to invest time, resources, and money with the right strategy. However, the processing of vast amounts of data can lead to unethical outcomes if not conducted following regulatory frameworks and not behaving in well-meaning.

For instance it has been given evidence of this phenomenon by the Facebook's case and the use of personal information to manipulate voters toward the desired outcome, and by the impact of superficial data processing activities for more vulnerable communities such as the cases in which, for example, most of the times, if a child is willing to search for female police officers, will be most likely disappointed with the results, as they will probably find the figure to be misrepresented.

As a matter of fact, I believe it is fundamental for such powerful companies to recognize their responsibility and to initiate a shift in the collective mindset and consider it a privilege to.

73. Custers, B., van der Hof, S., Schermer, B., & Appleby-Arnold, S. (2019). "A predictive privacy impact assessment: The case of profiling." *Computer Law & Security Review*, 35(1), 105324.

Tech giants may start adhering to best practices that not only aim at limiting the damages provided by their data processing activities, but rather start using their strength to positively influence the landscape, proactively adopting measures to avoid creating disproportionate injustices toward more vulnerable demographics, but rather creating a community created by data processors, data collectors, data subjects and third parties in which the trade-off is even, and all parties gain and give from the exchange.

Bibliography

Authors

- Altalex, R. (2019, January 24). *Art. 4 GDPR - definizioni*. Altalex.
- Barocas, S., & Selbst, A. D. (2016). *Big Data's Disparate Impact*. California Law Review, 104(3), 671-732.
- Boccaccini, P., Torresan, C., Boccaccini, P., Torresan, C., Boccaccini, P., & Torresan, C. (2023b, September 20). *Data valorization e data monetization, il dato quale asset strategico per il business: le sfide future*. Cyber Security 360.
- Custers, B., van der Hof, S., Schermer, B., & Appleby-Arnold, S. (2019). "A predictive privacy impact assessment: The case of profiling." *Computer Law & Security Review*, 35(1), 105324.
- Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. Basic Books.
- Narayanan, A., & Shmatikov, V. (2010). *Myths and fallacies of "personally identifiable information"*. Communications of the ACM, 53(6), 24-26.
- Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.
- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.
- Ofulue, J., & Benyoucef, M. (2022). *Data monetization: insights from a technology-enabled literature review and research agenda*. Management Review Quarterly. https://doi.org/10.1007/s11301-022-00309-1

- Parvinen et al., 2020
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, April 4). *Cambridge Analytica scandal fallout: Firm at center of Facebook storm closes*. The New York Times. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
- Solove, D. J. (2006). *A taxonomy of privacy*. University of Pennsylvania Law Review, 154(3), 477-560.
- Thomas and Leiponen, 2016
- Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*. Annenberg School for Communication at the University of Pennsylvania.
- Writer, G. (2023, September 4). *Ethics of data monetisation: Balancing personal privacy with economic value*. TheCable.

Legal References:

- Altalex, R. (2019, January 24). *Art. 7 GDPR - Condizioni per il consenso*. Altalex.

https://www.altalex.com/documents/news/2018/04/12/articolo-7-gdpr-condizioni-per-il-consenso

- Article 29 Data Protection Working Party. (2018). Guidelines on consent under Regulation 2016/679(WP259)
- Directive - 2002/58 - EN - eprivacy Directive - EUR-Lex. (n.d.).
- General Data Protection Regulation (GDPR) Article 32 - Security of processing. (n.d.). Retrieved from https://gdpr-text.com/read/article-32/
- General Data Protection Regulation (GDPR). (2018, March 29). *Art. 4 GDPR – Definitions*.
- General Data Protection Regulation (GDPR). (2018, March 29). *Art. 5 GDPR – Principles relating to processing of personal data*.
- General Data Protection Regulation (GDPR). (2018, March 28). *Art. 7 GDPR – Conditions for consent*.
- General Data Protection Regulation (GDPR). (2018, March 28). *Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject.*
- ICO. (n.d.). *Data sharing agreements*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/
- ICO. (n.d.-b). *Investigation into data analytics for political purposes*. https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/

- ICO. (n.d.). *Your right to get your data deleted*. https://ico.org.uk/for-the-public/your-right-to-get-your-data-deleted/#:~:text=The%20right%20to%20get%20your%20data%20deleted%20is%20also%20known,'right%20to%20be%20forgotten'.
- International data transfers | European Data Protection Board. (n.d.). https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en
- Privacy Impact Assessment - General Data Protection Regulation (GDPR). (2021, October 22). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/issues/privacy-impact-assessment/
- European Parliament. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Websites:

- *https://www.facebook.com/legal/terms/?paipv=0&eav=AfYcGnmXmKW18lUcoezaUtpQOSfH4Y7c_87ZwMoBxns6dFgIf_s25CYwgYnWeHLo25A&_rdr*
- *https://www.leonardo3.net/en/legals/cookies/*
- *Use of Cookies; Scientific American.*
- *. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en*

- *https://ico.org.uk/for-the-public/your-right-to-get-your-data-deleted/#:~:text=The%20right%20to%20get%20your%20data%20deleted%20is%20also%20known,'right%20to%20be%20forgotten'.*
- *https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en*
- *Unlocking financial benefits through data monetization, IBM Blog, February 19 2024.*
- *Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.*
- *https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/*
- *https://gdpr-info.eu/issues/privacy-impact-assessment/*
- *https://en.wikipedia.org/wiki/Facebook*
- *https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/#:~:text=In%202020%2C%20about%2097.9%20percent,increase%20in%20comparison%20to%20the*
- *https://blog.hootsuite.com/facebook-pixel/#:~:text=The%20Facebook%20pixel%20is%20a%20piece%20of%20code%20that%20you,of%20action%20on%20your%20website.*

- *https://sproutsocial.com/glossary/retargeting/#:~:text=Retargeting%2C%20also%20called%20remarketing%2C%20is,displaying%20ads%20or%20sending%20emails.*
- *https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/*
- *Facebook's Terms of Service and Privacy Policy: https://www.facebook.com/legal/terms/?paipv=0&eav=AfYcGnmXmKW18lUcoezaUtpQOSfH4Y7c_87ZwMoBxns6dFgIf_s25CYwgYnWeHLo25A&_rdr*
- *https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html#:~:text=But%20in%20Europe%2C%20some%20regulators,the%20company%20could%20use%20it.*
- *ttps://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0*
- *https://www.apiscene.io/api-security-identity/data-deletion-at-facebook/*
- *https://en.wikipedia.org/wiki/Cambridge_Analytica#:~:text=Cambridge%20Analytica%20was%20established%20as,royalty%2C%20and%20the%20British%20military.*
- *https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html*
- *https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal*

- *https://www.informationisbeautifulawards.com/showcase/3673-the-facebook-and-cambridge-analytica-scandal-explained-with-a-simple-diagram*
- *https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html*
- *https://news.cgtn.com/news/3063544f306b7a6333566d54/share_p.html*
- *https://oag.ca.gov/privacy/ccpa*
- *https://www.security.org/resources/detailing-delete-facebook-phenomenon/*
- Wikipedia contributors. (2024b, May 13). *Cambridge Analytica*. Wikipedia. https://en.wikipedia.org/wiki/Cambridge_Analytica#:~:text=Cambridge%20Analytica%20was%20established%20as,royalty%2C%20and%20the%20British%20military.
- Wikipedia contributors. (2024, May 5). *Facebook–Cambridge Analytica data scandal*. Wikipedia. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal