Hacettepe University Graduate School of Social Sciences

Department of Communication Sciences

Cultural Studies and Media

ALGORITHMIC CULTURE AND DATA ETHICS

Derya Güçdemir

Master's Thesis

Ankara, 2019

ALGORITHMIC CULTURE AND DATA ETHICS

Derya Güçdemir

Hacettepe University Graduate School of Social Sciences

Department of Communication Sciences

Cultural Studies and Media

Master's Thesis

Ankara, 2019

KABUL VE ONAY

Derya Güçdemir tarafından hazırlanan "Algoritmik Kültür ve Veri Etiği" başlıklı bu çalışma, 4 Şubat 2019 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

[İ m z a] Prof. Dr. [illegible]

[Unvanı, Adı ve Soyadı] (Başkan)

Prof. Dr. Mutlu BİNARK (Danışman)

[İ m z a]

[Unvanı, Adı ve Soyadı] Prof. Dr. Ruhdan Uzun

[İ m z a]

[Unvanı, Adı ve Soyadı]
Doç. Dr. Serhat KAYMAS

[İ m z a]

[Unvanı, Adı ve Soyadı]

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Musa Yaşar SAĞLAM

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- o Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- o Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ….. ay ertelenmiştir. (2)
- o Tezimle ilgili gizlilik kararı verilmiştir. (3)

27/02/2019

D. Güçdemir

Derya GÜÇDEMİR

[1] *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*

(1) *Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) *Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

(3) *Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Prof. Dr. Mutlu BİNARK** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

D. Güçdemir

Derya GÜÇDEMİR

DEDICATION

I would like to dedicate this thesis to my beloved grandfather and father.

To my grandfather Dursun ŞENSOY, who raised me from early age, took care of me as if I am his own daughter and prioritized young girls' education above anything else. I will be forever grateful for your love, hard work and sacrifices you did for me. You are our plane tree in this life and you will always be.

And, in memory of my father Ökkaş GÜÇDEMİR. I know that you would be proud, if you saw your little daughter who used to look at worms and insects in your science books, now completing her own first research. I am grateful for all the values you taught me.

ACKNOWLEDGEMENTS

This study could not have been completed without the support of my family, friends and my dear lecturers. I feel incredibly lucky to have you in this journey. And, I would like to take this chance to express my sincere thanks.

I would like to thank to my thesis supervisor Prof. Dr. Mutlu BİNARK for her endless help, support and consideration. I am specifically grateful to her for encouraging and believing in me even in those times when I was not able to speak the same language with her. This study has become a life-long learning experience for me thanks to her valuable supervising. I feel so proud to be your student and you have been my role model with your hard work, self-reflexivity as an academician and with your caring attitude.

I am thankful to members of the thesis jury Prof. Dr. Ruhdan UZUN and Assoc. Prof. Dr. Serhat KAYMAS for their valuable contribution and consideration.

I would like to express my thanks to Research Assistant Şule KARATAŞ ÖZAYDIN for her kind help, patience and support during this thesis study.

I would like to thank to my dear lecturers at Hacettepe University Communication Faculty for teaching me two important things: the importance of studying the mundane and questioning the background of every narrative.

My special thanks to Associate Prof. Hande ESLEN ZIYA. There are no words that can explain how grateful I am for your moral support and efforts that you have cultivated in me. Thank you for taking care of me as a person and also for guiding me as if I was your own thesis student! Thank you for reading, revising and discussing my thesis. You are my role model not only as an academician with your disciplined, hardworking and study enthusiastic attitude, but also as a woman by showing me to be fearless and to have courage to do what you love.

My biggest thanks are for my family. I am so grateful for all your support and love. Words cannot describe what it means to have you all in my life. Your presence made feel stronger and grounded. I am especially thankful to my mother Semiha GÜÇDEMİR for supporting me in everything that I ever wanted to do and wanted to be. I am so thankful to my brother Mehmet Deniz GÜÇDEMİR for being the most understanding and thoughtful brother ever! Many thanks to my cousin Ceyhun GÜLBAŞ for all the joy you bring into my life. You are my muse and you are the little brother that I have never had. I am thankful to my aunt Semra GÜLBAŞ for giving me strength and to my uncle Vedat GÜLBAŞ for supporting my education from a very early age.

I would like to thank my friends at Kitchen Republik, you have brought so much light into my life. Special thanks to my friends at Hacettepe -Özhan, Mine, Melis, Berke, Selin and Beril- for making my life bearable and not leaving me alone during this study. And, to Tolga GÜNTÜRKÜN and Burcu KARABAĞ for being the flowers of Ankara.

My special thanks to my soul sisters. Many thanks to my friend Irmak ALTINOK for being the sunshine in my life. I am so lucky to have you and thank you for enduring with me! Special thanks to my dear Zeynep KAYACAN for listening to me and being there for me, always! To my beloved Zeynep TOPCU BİLİR for her sisterhood and moral support!

I am so thankful to my friend Erol GUZOĞLU. Thank you for inspiring me to write my thesis on algorithms and data, and never leaving me alone ever since! Without your help and support, I know that I would never be able to do any of this. Not only your moral support, but also your technical expertise helped me to overcome difficult times on the road. I am so grateful for everything you have done for me!

And, I truly know that if this thesis is an achievement, it is not mine, but all of yours.

Lastly, I also would like to thank all the woman who paved the way for us younger generations to do what we love.

ÖZET

GÜÇDEMİR, Derya. *Algoritmik Kültür ve Veri Etiği*, Yüksek Lisans Tezi, Ankara, 2019.

Bu tez çalışması, sosyal ağlarda ve İnternet'te çalışan algoritmaların özelliklerinin kültürü ve toplumu nasıl etkilediğini incelemektedir. Bir zamanlar temel olarak Bilgisayar Bilimlerinde tartışılan algoritma şu anda gündelik yaşamın içinde tartışılan bir konu haline gelmiştir. Algoritmalar daha önce var olsa da teknolojik kapasiteleri ve yaşamın çeşitli alanlarına uygulanmasından dolayı ortaya çıkan sosyal ve kültürel etkileri hakkında yeni tartışmalar mevcuttur. Bu açıdan, araştırmanın ana ilgi alanı algoritmaları yeni bir inceleme alanına neyin dönüştürdüğünü, neden sosyal bilimlerdeki tartışmaların bir parçası haline geldiğini ve günlük yaşamın akışı içinde ve aktivitelerinde nasıl öne çıktığını bulmaktır. Modern enformasyon toplumlarında, kültüre ait olan görevler giderek artan bir şekilde bilişimsel süreçlere verilmektedir ve bu durum *Algoritmik Kültür* olarak tanımlanmaktadır (Striphas, 2015). Bu değişimin, bilgi diyeti, algoritmaların ekonomi politiği ve gözetim olarak kavramsallaştırılabilecek sosyal, kültürel ve ekonomik sonuçlar yarattığı düşünülmektedir. Kültüre ait olan görevlerin bilişimsel süreçlere atfedilmesiyle ortaya çıkan kültürel, sosyal ve ekonomik sorunlara cevap vermek için, bu çalışma veri etiğini önermektedir. Bu bakımdan, veri-güdümlü algoritmalardan ve veri pratiklerinden dolayı ortaya çıkan sorunları, algoritmaların özelliklerini ve çeşitlerini içeren bir etik harita oluşturulmuştur. Harita, etik problemleri kavramsallaştırmayı ve bu sorunları örneklerle ampirik olarak tartışmayı amaçlamaktadır. Çalışma, sorunlar için düzenleyici cevaplar önermekte ve 'etik dışı' olan sabitlenmeden önce bir etik tartışma başlatmayı amaçlamaktadır.

Anahtar Sözcükler

Algoritmik kültür, veri etiği, etik, algoritma, veri

ABSTRACT

GÜÇDEMİR, Derya. *Algorithmic Culture and Data Ethics*, Master's Thesis, Ankara, 2019.

This thesis study examines how features of algorithms that run on social networks and on the Internet affect culture and society. Algorithm which was once mainly debated in Computer Sciences has now become a topic of everyday life discussions. Even though, algorithms did exist before, there are new discussions surrounding them about their societal and cultural impact, emerging from their technological capacities and their application on various areas of life. In this respect, the main interest of this research is to find out what makes algorithms a new concern, why they become a part of the debates in social sciences and how they become prominent in the flow and activities of daily life. In modern information societies, the works of culture are increasingly being handed to computational processes which is called as *Algorithmic Culture* (Striphas, 2015). It is thought that this change has created social, cultural and economic outcomes which are conceptualized as information diet, economy politics of algorithms and surveillance. In order to deal with cultural, social and economic problems emerging from attribution of culture's work to computational processes, this study suggests data ethics. In this regard, an ethics map is created including problems rising from data-driven algorithms and related data practices, features of algorithms and types of algorithms. The map has the purpose to conceptualize ethical problems and to discuss them with case studies empirically. The study suggests regulatory responses for the problems and aims to initiate an ethics discussion before the 'unethical' is stabilized.

Keywords

Algorithmic Culture, data ethics, ethics, algorithm, data

TABLE OF CONTENTS

ABBREVIATIONS

ACLU: American Civil Liberties Union

AMA: Artificial Moral Agent

AOIR: Association of Internet Researchers

BRIC: Boston Regional Intelligence Center

CFPB: Consumer Financial Protection Bureau

DPI: Deep Packet Inspection

ESOMAR: European Society for Opinion and Marketing Research

FB: Facebook

FICO: Fair Isaacs Corporation

GDPR: General Data Protection Regulation

GFT: Google Flu Trends

HTML: Hypertext Markup Language

ICT: Information and Communications Technology

ISP: Internet Service Provider

NGO: Non-Governmental Organization

OSPs: Online Service Providers

SCS: Social Credit System

SEO: Search Engine Optimization

SIIA: Software & Information Industry Association

USA: United States of America

WHO: World Health Organization

TABLES

LIST OF FIGURES

INTRODUCTION

This thesis titled *Algorithmic Culture and Data Ethics* investigates how features of algorithms that run on social networks and on the Internet affect culture and society. Algorithm, once belonged to Computer Sciences has become a major topic for everyday life discussions. Though algorithms did exist before, now the recent discussions surrounding them are more and more about their societal and cultural impact, emerging from their technological capacities and their application on various areas of life. In this respect the main interest of this research is finding out what makes algorithms a part of the debate in social sciences and how they become prominent in the flow and activities of daily life.

Algorithms concern people, academics, companies as well as governments mostly because data have become one of the main economical input of information societies. In fact, more and more parts of our lives have become digital and people continue providing a great amount of data about their actions by using digital devices and applications to do business, to shop, to eat, to communicate, to entertain and to fulfill many other works. Whenever a person uses a digital device, s/he leaves digital trails behind which are narratives telling *stories* about them. Digital trails are considered as key to who the person is, what s/he does, likes, prefers and what s/he searches or looks for. And, algorithms which are capable of mining user data, learning from data and making predictions out of the data have become important tools for individuals, companies and governments to create insights, to make decisions and to answer questions for them in an efficient way. This is possible, because algorithms have two important characteristics: *logic* about how they operate and *control* on how they run the data.

In modern information societies, computation on social networks and on the Internet is used to develop sophisticated features for algorithms. People experience different types of algorithms working on their digital devices and life such as ranking, profiling, tracking, recommending, filtering and etc. These algorithms are working on both *through* human subjects and objects shaping ideas, way of thinking, habits, preferences and tendencies. And, these kinds of actions of algorithms are possible, because their features are autonomous, decision-making and value laden. As a result, what is experienced today is that people are using algorithms not to have logic and control on how to produce goods, but to help them to answer more *subjective* questions and to make more *complex* decisions such as who should I fall in love with, what should I read, watch and listen, which transportation should I use to reach from A to B, what is important and what is not (Tüfekçi, York, Wagner & Kaltheuner, 2015, p. 6)? Once these subjective and complex questions are given to algorithms, in fact the work of culture is being handed into algorithms. This phenomenon which occurs with regard to these digital processes is called as *Algorithmic Culture* (Striphas, 2015). Following the concept of *Algorithmic Culture,* this thesis suggests that algorithms should not be seen as technical assets consisting of data and code but as algorithmic culture, where they act as social and technological *assemblages* (Ananny & Crawford, 2016, p. 11). In other words, in this algorithmic culture, one's experiences and everyday practices related to data-driven algorithms will be traced.

When we argue that algorithms shape how and what people experience, then we must ask how in return they regulate the very life one lives in. In this respect it is discussed that decision-making, learning, gate-keeping, micro-targeting, prioritizing, opaque and autonomous features of algorithms grant them *power* to regulate relations, practice and human conduct. Humans benefit from the features and capacities of algorithms which bring more efficiency into life. However, there are also *bad practices* of data and algorithms, because no company or government can say 'no' to such a power which is indicative of people's actions and which is loaded with meaning and inferences from human life. Based on such assumptions this thesis will question and try to understand: what is at stake with the algorithmic power, what are the bad practices of data-driven algorithms, what are the unethical results rising from the features of algorithms and data practices and how can we address them, and what can be done to prevent companies or governments to abuse, commodify and commercialize personal data?

This research will underline the importance of studying ethics of data. By ethics, morality of the emerging problems will be discussed. Data ethics is selected for this study, because it is inclusive of ethical problems pertaining to data, algorithms and its relevant practices. Ethical thinking is considered as a key for the solutions of the emerging problems. If a change is desired in a society, then the ethical thinking is the first thing that needs to be developed, because ethics which is bound to culture and society regulates how people think, behave, act and produce. It is discussed that studying ethics of data can lead to more responsible and accountable practices of data, increase human agency, control and access with regard to data against private companies and governments and bring better practices of data which can lead to more benefit from the capacities of algorithms.

The *aim* of this thesis is to understand impacts of algorithms which work on social networks and on the Internet into social life and culture. This study aims to understand algorithmic culture, its properties and its role in experiencing culture in everyday life. This study aims to reveal ethical problems emerging from features of algorithms and related data practices before the debate is closed to discussions. In order to achieve this, the study starts an ethics discussion which is considered as a solution for the emerging problems. By questioning morality, agency, responsibility and accountability of machines and algorithms, the study aims to find a path to study ethics of data and to find out what ethical algorithm means. For this reason, the study creates an ethics map which addresses the ethical problems, features and types of algorithms. The ethics map has the purpose of framing the discussions around the unethical practices of algorithms and will be one of the major inputs of this thesis. At the same time, it will not be a remedy or panacea for the problems. But it will serve as a map to illustrate the existing ethical dilemmas and from time to time will help us show the hidden and unseeable ethical problems. At the end of the study, regulatory responses are developed for the ethical problems with the purpose of exemplifying what can be done to prevent disparate impact of algorithms and unethical practices of companies and governments.

In this respect this study will aim to tackle with the following research questions:

- How do digital algorithms pertaining to Computer Sciences become a subject of Cultural Studies? In other words, what are the features and capacities that make algorithms a new concern?

- What kind of relations do algorithms create between culture, people and technology?

- How do algorithms interact with culture? What is the role of data-driven algorithms in experiencing culture in daily life?
- What is the difference between human decision-making and computer decision-making? How can the notion of morality, responsibility and accountability be discussed in relation to algorithmic agency?
- What kind of power do algorithms have? What kind of power relations do algorithms create between people, companies and governments? What are the tensions between human and non-human?
- What are the impacts of algorithms into culture and social world? What are the ethical problems arising from the algorithms?
- What is at stake when we say algorithmic judgement and decision-making? What does it mean for an algorithm to be definer of culture in relation to delivery of information and content on OSPs?

In doing so, the study will focus on ethical problems emerging from features of algorithms before the debate is closed to discussions.

The *main problem* of this study is that algorithms and algorithmic data have become definers of cultural field and social life with their value-laden, autonomous and opaque nature which have decision-making, gate-keeping, prioritizing and micro-targeting features. These features make algorithms a new concern in information societies whose main input is data. Data-driven algorithms create unethical practices with regard to delivery of information, economy politics, surveillance which require studying data ethics as a response.

The first sub problem is that algorithms have features to filter information, to profile people, to recommend content, to regulate human relations, to personalize social networks and search engines. It is discussed that this leads to an appetite of consumption and narrowing of world views.

The second sub problem is that data are sold, commodified, exploited, abused, traded and shared with companies, third parties and governments to target advertisements and to gain more profit. It is discussed that this leads to commercialization and commodification in an abusive way.

The third sub problem is that data practices of companies and governments to keep track of people's digital data create ethical issues about person's privacy, right to privacy, control and access to personal data. It is discussed that this leads to dataveillance, loss of agency, loss of privacy and control.

The fourth sub problem is that opaque and autonomous algorithms can make decisions regarding human values and life in a discriminative, edited, omitted, personalized and biased way. However, it is realized that there is not enough discussion in the field about how data ethics should be studied and applied and what ethical perspective should be. Therefore, this study suggests that studying data ethics can lead to more ethical practices of data-driven algorithms at individual, corporate and governmental levels.

The *research question* of the thesis is what are the effects of data-driven algorithms on culture, cultural practice and social life and how can ethical problems rising from the features of algorithms and data practices of the parties be addressed?

The *scope and limitations* of this study is based on online service providers (OSPs). This study examines and analyzes impacts, features and types of algorithms only when they are performed on social networks and on the Internet provided by OSPs such as (including but not limited to) Google, YouTube, Facebook, Twitter etc. The study specifically examines algorithms which are computational, subjective and complex, whose nature is hard to comprehend and which are value-laden, autonomous and opaque with capacities of decision-making, learning, prioritizing, micro-targeting and gate-keeping. For instance, algorithms which are used in production of goods are not within the scope of this study. In the first chapter, the study approach surveillance studies only from the point of dataveillance, as this thesis has a specific concern on the usage of personal data. Other types of surveillance are beyond the limits of this study. In the second chapter, foundations of the ethics discussion are based on deontological, teleological and virtue approaches. Other ethical approaches are not included, as they are not considered as workable for the purpose of this thesis. How algorithms impact social life and culture is examined with case studies which emerge on OSPs. Other examples related to impact of algorithms and algorithmic systems outside the realm of OSPs are discussed in footnotes which are considered as enlightening.

The *method* of this thesis will be thematic analysis of the academic literature published on data ethics and algorithmic culture. However, the analysis of the literature will be supported with the media and ethics theories[1]. Such analysis of the existing theories and literature will help discussing and analyzing what algorithmic culture is, what ethics is, what could rise from being 'unethical' and how ethics can be considered as a solution for the emerging problems. In order to examine the impacts of algorithms into social life and cultural field, ethics map is developed as a tool to make ethical problems visible. The theoretical discussions surrounding algorithmic culture are supported with case studies empirically. In this way, the discussion is enriched with prominent examples of algorithms creating unethical results.

The *importance* of this study is that understanding data-driven algorithms, their features and capacities provides new ways of understanding information societies and problems people experience in digital modern societies on daily basis. The study tries to develop ethics for algorithmic culture before every part of digital life is abused. The study tries to draw attention to questions how algorithms operate and what their practices mean. Being the first thesis study on algorithmic culture in Turkey[2], it will –hopefully- contribute to field at different levels. Studying algorithmic culture and its ethics is thought to have more importance in the coming years as more parts of offline life will become online, more devices will communicate with each other and more companies

[1] In the first chapter these theories are: *Algorithmic Culture* by Ted Striphas to explain how cultural practices are assigned to algorithms and algorithmic systems: *Networked Information Algorithm* by Mike Ananny to understand algorithmic systems as assemblages of human and non-human agents: *Filter Bubble* by Eli Pariser to understand impacts of personalization for the sake of relevancy: *Eco Chambers* by Cass Sunstein to understand group polarization on social networks: *Critical Political Economy* by Christian Fuchs to understand ecology of OSPs and the Internet: *Panopticon* by Michel Foucault to develop a perspective for surveillance on social networks: *Dataveillance* by Roger Clarke to emphasize tracking and monitoring of personal data. The theories and concepts that are used in the second chapter are: *Deontological Ethics* approach by Immanuel Kant to understand that it creates the basis of codes of conduct: *Teleological Ethics* approach by Jeremy Bentham and Stuart Mill to understand that it enables reflections for the outcomes of the technology; *Virtue Ethics* approach by Aristotle and Rosalind Hursthouse to understand the importance for a technologist to have traits for ethical flourishing: *Impact Model of Ethics* by Annette N. Markham to create insights for the possible impacts of the technology.

[2] When "data ethics" and "algorithmic culture" are searched on the thesis center of Council of Higher Education, no matching results are found at the web site https://tez.yok.gov.tr/UlusalTezMerkezi/.

and governments will look for the ways of making use of personal data. Therefore, it is believed that this thesis study is important in terms of drawing attention to data ownership, privacy, economic value of data, and to the question of how data are used in general. The study can be considered as a step to develop an ethical thinking for algorithms. That is to say, this study is believed to be important in terms of paving the way for ethical discussions about algorithms and trying to find ways to make parties in the algorithmic system more accountable and responsible. Because it is believed that ethics can become regulations and law, making data holders and data rich companies/individuals -at institutional and individual level- more accountable and responsible for their actions.

This thesis study consists of two chapters and the thesis outline will be as follows. In the *first* chapter, properties of algorithmic culture which leads it to become a new concern and its relations to culture, society and Cultural Studies are explained. After reviewing the literature on algorithmic culture, it is suggested that discussions surrounding the algorithmic culture can be conceptualized and analyzed in three discussion categories: information diet, economy politics of algorithms and surveillance.

Information diet suggests that proprietary algorithms of companies do not only constitute the platforms that people search information, socialize or interact, but they also affect how information is delivered, which information is delivered to whom, how information is edited and omitted on search engines and on social networks. Information diet is designed under three tittles which are *personalization, filter bubbles* and *echo chambers.* Personalization explains how search engines and social networks are personalized according to each user, how everyone has their own Google or newsfeed, how different people get different search results and how similar content is recommended to users for the sake of relevancy. Filter bubble explains how people started living in bubbles that are similar to their own thanks to personalization algorithms, how people are connected with individuals more whose ideas that they hold dear and how this situation limits their world view. Eco chambers explains how culture transforms from being confronting to conforming (Hallinan & Striphas, 2016, p. 122) and how group polarization on social networks emerge.

Economy politics of algorithms focuses on why data are valuable, why data have economic value, why it is considered as the new oil in information societies. Economy politics of algorithms is designed under the three titles which are *platformization and dominance of OSPs*, *targeted ads* and *behavior market.* Platformization and dominance of OSPs examines ecology behind these platforms, economic incentives and structures. Targeted ads examine how advertisement has become the backbone of the OSPs and business structure of platforms, how data are used in order to target ads to specific users. Behavior market examines how tracking of user data and behavioral targeting monetize relations and habits.

Surveillance examines how data and algorithms are used for tracking and monitoring practices, how these practices create value for the parties that surveil. Surveillance is designed under three titles *Reversing the Panopticon*, *Dataveillance* and *Privacy, Control* and *Access.* Reversing the Panopticon inspect what theory of Panopticon means on social networks and on the Internet, how Panopticon is reversed at a time of 'shares & likes' and how surveillance is normalized. Dataveillance examines the impacts of tracking personal data, how it leads to disempowerment, power asymmetry and discrimination. Privacy, access and control questions what right to privacy means, who should own data and who should access and have control over data in order to create a balance between users, companies and governments and also to restore imbalances between the three.

It is discussed that data-driven algorithms are creating ethical problems due to their features, capacities and their usage by companies and governments. Therefore, the study suggests studying ethics of data for the emerging problems. The *second* chapter Data Ethics has the purpose to be an answer to the question what should be done for the ethical problems that arise in algorithmic culture. The ethical problems are defined and conceptualized as *invasion of privacy, discrimination, bias, automation, ossification, manipulation, asymmetry, appetite of consumption, data ownership, consumerism* and *commercialization.* It is first discussed that deontological, teleological and virtue approaches are considered as workable to analyze the ethical problems. They constitute the basis of the ethics discussion in this study. However, data ethics is adopted, because of six emerging problems in socio-technological assemblages which are *hyper* *connected* and *networked* power relations, *concept of agency, knock-on effects, knowable outcomes, unstable nature of algorithms* and *the problem of many hands.* It is argued that data ethics is comprehensive of handling these problems. Afterwards, meaning of an ethical algorithm is discovered by questioning of morality, responsibility and agency of machine agents. It is discussed that machine agents can have *functional moral responsibility* (Dodig Crnkovic & Çürüklü, 2012) in order to understand their regulatory role, as long as they are considered as parts of socio-technological assemblages in which responsibility is distributed between human and non-human agents. The ethical approach of this study requires social and cultural practice as morals and decisions, but also codes of conducts, regulations and responsibility for the outcomes of the technologies and reflections for the design and practice of algorithmic systems. This study offers regulatory responses for the ethical problems which are *accountability, transparency, notification* and *direct regulation of governments and institutions*. This chapter of the study concludes that as much as we need institutions to regulate, enforce and control practices of individuals or companies that are powerful in the algorithmic systems, we need ethical understanding itself to flourish in order to develop technology for the society. And, this will require to understand the society, its problems and its Geist in the first place.

At the conclusion, considerations on how ethics can flourish in the society will be discussed with suggestions. Besides, the situation in Turkey with regard to data, algorithms and related practices of government and companies will be reviewed and argued with examples.

CHAPTER 1

ALGORITHMIC CULTURE

"Algorithmic judgement is the uncanny valley of computing"

– Zeynep Tüfekçi (2014).

Imagine there is a girl. This is her experience with algorithmic culture and she has a story to tell. One day, she and one of her friends were searching for information on one of the most used search engines Google, sitting next to each other. Then, they realize that the results they get are different from each other, even though they search the same subject with the same key words. How was it possible that they have their very own Google? They soon realized that their searches were personalized for the sake of relevancy. They felt like they are living in different realities and having a diet on information.

The next day, she was searching "why LGBT…" and then the search engine autocompleted the sentence with "should not be taught at school", whereas she was actually looking for "why LGBT rights are important". She was confused with where this assumption came from and why the search engine autocompleted her query in a biased way. She was curious to understand the reason. She later found out that there was nothing new! It was an old wine in new bottle matter. Autocomplete was based on the real searches people make on the search engine. She realized that the predictions were coming out of the society. The autocompletion of the search engine was a reflection of the world, nothing new.

Elections were coming soon and her Facebook newsfeed were full of news and posts about politics. However, she realized that she was seeing some of her friends' posts more than others. She started not hearing from them and she was wondering if they were not active on social media anymore. She had no clue what they were doing. However, she soon realized that people that she sees on her newsfeed were the ones that she holds dear, liked, commented and interacted. This was telling her a story about how this platform was functioning. She was not hearing from people with whom she had little in common, even though she was very interested in what they share – their worldview. She felt a little disconnected, passive and closed to her own circle of friends and limited to her own world. However, she was hoping for diversity and it was getting boring. Where did the platform get the assumption that she would be happy to see posts of likeminded friends? Why did it decide on behalf of her? However, this was narrowing her world view and it was reductive in a sense, as she was closed to outer impact and interaction by not coming across with counter ideas. Also, she realized that this was a perfect way for platforms to keep their users engaging –resulting in production of more data for them.

The next time, she was searching meditation music for her yoga practice on YouTube. After having found what she was looking for, it kept recommending her similar videos ranging from ten minutes guided meditation, best meditation practice to inspirational Ted Talks claiming to know the key to happiness, balance and health. The more she got curious about what these people have to say, the more she spent her time on YouTube. She already knew about the recommending feature of YouTube. But, how did it know what she *exactly* needed and what would *truly* interest her? Similarly, she was getting e-mails from different web sites asking her, if she is *still curious about* the topic she was reading yesterday or they were showing her new articles similar to her research areas. It was not long that she realized her need for a healthier, balanced and meaningful life was commercialized and her quest for information was abused in a sense. These platforms were not innocent to recommend her similar content, one video or article after another, but they were aiming to maximize the time she spends on their platform, keeping her online with the content that is most *relevant* to her. This time she realized that not only her need, but also her *attention* and her *focus* were interrupted and became a part of the economy.

Another day she was looking for flight tickets to İstanbul for her holiday. After looking at one or two, she decided not to purchase and left the web site. Afterwards, she visited an online dictionary web site and found out that her flight search was being marketed to her. The flights haunted her through the web. They were literally everywhere she paid a visit! How was it possible that her search for İstanbul flights were known by every web site on the Internet and even on her social networks? After trying to understand the logic behind, she found out that it was behavioral targeting and remarketing strategy of Google to remind her to make the purchase!

And a year later, she was talking out loud about a product near her phone. Afterwards, it showed up as targeted ads on her social media account. How could social networks target the product even when she did *not* look for it online? She was a hundred percent sure that she did nothing online, but simply talked about the product near her phone. She starts guessing that was her mic on? If yes, which application had the permission to do it so? Or, was it a perfect creepy coincidence? Or, was she just too crazy? She already learnt that companies were making use of her data to target ads based on previous behaviors such as her clicks, location data and searches on the Internet and social media platforms. However, she also read that most of these technology giant companies claim that they do not use mic to listen their users in order to target personalized ads. So, how was this possible? Where did this creepiness come from?

Thus, what was happening here? How do computer systems become so decisive in various processes that are related to human life and culture? How do they become so predictive? What are the features that enable them to act as decision-makers and gate-keepers? How do they infer meaning from human life so accurately? What was the importance of it?

What is observed is that data-driven algorithms are making decisions for us, with us and through us. It is believed that as users, citizens and individuals, people are experiencing the effects of deployment of algorithms into cultural practices more and more. This is a new era where computing systems are not only used to make calculations for us, but to decide what is important, relevant and best for us -answering more subjective and complex questions- (Tüfekçi, 2014), and this thesis calls this new era *Algorithmic Culture*, following the steps of Striphas. For some, these implications may seem like magic. For some others, they can be regarded as creepy or intrusive. However, we need to be compatible with the emerging practices of algorithms. And, it is believed that in order to achieve that we first need to understand what algorithmic culture is.

1.1. UNDERSTANDING ALGORITHMIC CULTURE

In this section of the thesis study, terms and questions constituting the algorithmic culture will be explained. This part aims to answer these questions; what is algorithm, what are data, what is “new” about data and algorithms, which algorithms is this study interested in, why has algorithm become a subject of daily life discussions, what is algorithmic culture, and what is the relation of algorithms to culture and in generally to Cultural Studies?

1.1.1. What is Algorithm?

“Algorithm = Logic + Control”[3]
(Kowalski, 1979, p. 424)

According to software and computer studies, algorithm can be considered as consisting of a logical and a control component. Logic component specifies the knowledge which is to be used in solving problems. And control component is the one determining problem-solving strategies with which this knowledge is used (ibid). As Goldschlager and Lister argued (1988), it is a “description of the method by which a task is to be accomplished” and it is “the unifying concept for all activities which computer scientists engage in” (as cited in Goffey, 2008, p. 15).

Algorithm, in its contemporary meaning is regarded as formal processes, procedures or set of steps which are generally expressed mathematically (Striphas, 2015, p. 403). According to Gillespie, algorithms do not need to be software, in a very broadest sense, “algorithms are encoded procedures for transforming input data into a desired output, based on specific calculations” (Gillespie, 2014, p. 167).

Algorithms have important role in computing systems and software both theoretically, practically and ideally; they are not only belonging to mechanical and computational discourse, but they are also belonging to social, cultural and economic field. Because none of the abstraction related to algorithms tells much about the social, political and cultural role algorithms play (Goffey, 2008, p. 15). And this thesis aims to reveal this.

[3] In this thesis study, the control factor in algorithms is associated with the societal effects and impacts due to power inherited in their inner working systems.

1.1.2. What are Data?

As Andrew Goffey argues “algorithms obviously do not execute their actions in a void. It is difficult to understand the way they work without the simultaneous existence of data structures, which is also to say data” (Goffey, 2008, p. 18). Data are considered as a raw material which is produced by abstracting the world into forms such as numbers, symbols, characters, images, bits etc. through which information is created (Kitchin, 2014, p. 1). This data can be found in nature as representative (such as a person’s weight, opinion, habits etc.), implied (via absence) and derived (data that are produced from other data). Data can be recorded and stored in analogue or digital form (ibid).

According to Kitchin, data which have utility and value provide inputs to the various analyses which are used by individuals and institutions to make sense of the world (ibid). And in turn, these are used “to create innovations, products, policies and knowledge that shape how people live their lives” and in this sense, data have become a key source (ibid).

Data can be categorized into three as structured, semi-structured and unstructured. Kitchin define structured data as data which “can be easily organized, stored and transferred in a defined data model” (ibid, p. 5). Structured data are considered as data which “can be processed, searched, queried, combined and analyzed relatively straightforwardly using calculus and algorithms” (ibid). On the other hand, semi-structured data are the ones whose structures are “are irregular, implicit, flexible and often nested hierarchically” (ibid). They are described as “loosely structured data that have no predefined data model /schema, and thus cannot be held in a relational database” (ibid). And finally, unstructured data defined as the data which “do not have a defined data model or common identifiable structure” (ibid). Unstructured data “can be searched and queried, but they are not easily combined or computational analyzed” (ibid, p. 6). However, they can “be converted into structured data through classification and categorization” (ibid).

1.1.3. What is 'New' About Data and Algorithms?

Data and algorithms have always existed, they are not new phenomenon. However, people –as being users or producers- experiencing something that feels quite "new", because how they experience data has changed. A question that needs to be asked maybe is that "is this merely 'old wine in new bottles' or are there genuinely new issues related to patterns of algorithmic design as they are employed increasingly in real-world applications" (Burrell, 2016, p. 2)?

And in information societies[4] of the modern world that people live in, four major developments have taken place which changed people's experience of data and algorithms into something "new". As Burrell has suggested what is *new* in this domain is "the more pervasive technologies and techniques of data collection, the more vast archives of personal data, an outcome of more universally adopted mobile devices, services and applications and the reality of constant connectivity" (ibid). That is to say, people are producing data more than ever before, as nearly all of their everyday activities –from communication to entertainment- carried out with computational devices based on algorithmic designs.

Therefore, the word algorithm and data has been going through a shift in their public presentation, they are changing from being technical issues into terms which are attached with a polarized discourse among public (ibid). As Gillespie suggested, it is also because people are making computational tools as their main media of expression, and making all information digital which means that people prefer to subject human discourse and knowledge to those procedural logics which supports all computation (Gillespie, 2014, p. 168).

Consequently, how data and algorithm are defined is changing, too. It is because their function is also subject to change. In information societies, data are considered as an important power, because data can enhance economy, contribute to science and well-

[4] As defined by Van Dijk, information society is a social organization that is based on science, rationalism and reflexivity; an economy whose sectors and values are increasingly defined by information; a labor market which is based on information processing; a culture which is governed by media and information products which have its own signs, symbols and meanings (Van Dijk, 2006, p. 19).

being of people, but it can also lead to manipulation, bias and tracking. Therefore, algorithm which are operating on these data "are not just codes with consequences, but at the latest, they are socially constructed and institutionally managed mechanisms" (Gillespie, 2014, p. 192). That is to say, algorithms are running the data individuals provide to them. As there is a human touch, the data will be fed and nourished from the society it emerges. In order to make sense of the patterns that data create, the analysis of the data will be institutionally managed such as governments or private companies. As a result, the algorithms are not only considered as automated coded consequences, but they are socially created and managed. That is to say, the data algorithms operate will reflect the society.

1.1.4. Which Algorithms is This Study Interested in?

In order better understand this change which is turning the phenomenon from being a technical issue into something socio – technological, it is important to scrutinize which algorithms are at play in information societies. The algorithms that this research is interested are the ones "whose actions are difficult for humans to predict or whose decision-making logic is difficult to explain after the fact" is assigned (Mittelstadt, Allo, Taddeo, Wachter & Floridi, 2016, p. 3). That is to say, the algorithms which carry out mundane tasks such as algorithms used in manufacturing are not concern of this study (ibid). It can be further outlined that the "algorithms which makes generally reliable (but subjective and not necessarily correct) decisions based upon complex rules that challenge or confound human capacities for action and comprehension" are the attention of this study (ibid).

This study is into computational and digital algorithms which have the *power* to create social, cultural and economic phenomenon and which emerge "sociological and normative features" (Ananny, 2016, p. 97). This means that decision-making, semi-autonomous, value-laden and opaque algorithms and also machine-learning algorithms are the concern of this study. It is because of the fact that these algorithms have the features and the *power* to sort, rank, filter, recommend, profile and target subjects and objects among one another. The examples include Facebook's ranking algorithm which prioritize one content over another in the newsfeed of people; sorting algorithms which are similar to ranking algorithms deciding which content to be shown based on relevancy; YouTube's recommending algorithm which suggest *related* and similar content based on previous views; targeting algorithms which hunts users through the web and micro-target the content for specific users to make them buy goods based on their clicks, searches and habits crawled by cookies; profiling algorithms which creates demographics, geographics and psychographics of people by mining their data; filtering algorithms of social networks deciding which information or post to be visible to users based on their world views and interactions with other people and likes. As David Beer suggests, the society is witnessing "a power through algorithm" (Beer, 2009, p. 985). The power that algorithms have is not a hegemonic power which is imposed by external organizations, it is rather a power that can be called as "post-hegemonic" where "the hegemon has moved out into the everyday and power operates from the inside rather than from above" (Beer, 2009, p. 991; Lash, 2007).

The features of these algorithms, what they cause in the socio-technological sphere and the problems that come along with them will be examined in detail in the ethics discussion.

1.1.5. Why has Algorithm Become a Subject of Daily Life Discussions?

Algorithm, which was once belonged to computer science now has been a subject of everyday conversations and discussions. Their effects are increasingly being discussed in media outlets, academy, political discourse and social media platforms; people started discussing it in their everyday life practices. Thus, it is important to answer and understand how algorithms take active role in everyday life.

It actually stems from the fact that "when digital processes become more visible as elements that shape our experience, then algorithms in particular become part of the conversation about how our lives organized" (Dourish, 2016, p. 1). That is to say, boundaries of the term algorithm are not determined by technological constraints, but rather by social engagements (ibid, p. 3).

Couldry (2012) argued that although algorithms are abstract tools related to computation, they are created to be embedded in the real word in which information is processed and users live in (as cited in Gillespie, 2014, p. 183). They have nestled into daily lives and mundane practices of people, influencing how people search information, how they perceive and think about knowledge and how people understand their existence in and though public discourse (ibid). In the contemporary world of the information societies, decisions and choices which were once belonged to humans have been increasingly given to algorithms advising how to interpret data and what kind of actions to take; and this means that algorithms are mediating digital life and decision-making (Mittelstadt et al., 2016, p. 1).

Personal data people produce and digital traces people leave behind are subject to networked connected and advanced capitalistic societies on daily basis (Burrell, 2016, p.1). Striphas (2009) suggested that every day and cultural activities are now data-driven which are subject to machine-based information processing (as cited in Striphas, 2015, p. 398). That is to say, as Dodge and Kitchin argued, “software is increasingly making a difference to the constitution and production of everyday life” (2009, p. 1344). And “the implications of software are ‘sinking’ into and ‘sorting’ aspects of our everyday lives” (Beer, 2009, p. 985).

Therefore, algorithms and their decision-making, value-laden and semi-autonomous structure start regulating social order, shaping how information is consumed and how realities are constructed. Various daily life activities and media consumption – such as online news selection, consumption of music, film and video entertainment- have been shaped by automated algorithmic selection via search engines and recommending systems (Just & Latzer, 2017, p. 239). Algorithmic selection (of things) is making them an important determinant in information societies, because algorithmic selection shapes individual’s realities and consciousness, and in turn, this influences societies’ culture, knowledge and values (their realities and consciousness) and as a result, it affects social order in contemporary societies (ibid, p. 246).

1.1.6. What is Algorithmic Culture?

Algorithms are taking active role in communication, consumption and everyday life practices beyond –people and producers’- comprehension and control. And it seems that we are kind of lacking of a vocabulary which can name, assess and help us to understand the *intervention* of these algorithms (Gillespie, 2012). As Ananny (2011) argues, “we don’t have a language for the unexpected associations algorithms make, beyond the intention (or even comprehension) of their designers” (as cited in Gillespie, 2012).

It is important to realize that the word algorithm has been lately used as an adjective instead of a noun, such as “‘algorithmic identity’ (Cheney – Lippold, 2011), ‘algorithmic regulation’ (O’Reilly, 2013), ‘algorithmic power’ (Bucher, 2012), ‘algorithmic ideology’ (Mager, 2012), ‘algorithmic turn’ (Uricchio, 2011), or the “algorithmic culture” (Striphas, 2010)”, emphasizing a social and cultural phenomenon which is driven by and attributed to algorithmic systems (Gillespie, 2016, p. 25). These algorithmic systems do not “include just algorithms themselves, but also the computational networks in which they function, the people who design and operate them, the data and users on which they act, and the institutions that provide these services” (ibid). That is to say, algorithmic systems are not only made of codes and they do not operate own their own; there are more actors involved which build up the algorithmic culture. These agents range from networks to people, from data to institutions.

This thesis study is taking the definition of Ted Striphas’s *Algorithmic Culture* to explain the emerging social phenomenon. According to Striphas, algorithmic culture means “delegating the work of culture – the sorting, classifying and hierarchizing of people, places, objects and ideas”, and also the habits of thought, conduct and expression increasingly to computational processes (Striphas, 2015 p. 396; Hallinan & Striphas, 2016; Galloway, 2006). Hallinan & Striphas ask a very important question which constitutes the main problem of this study; “how does algorithmic information processing affect the meaning of the word *culture*, and, by extension, cultural practice” (Hallinan & Striphas, 2016, p. 117)? In order to answer this question, this thesis study will look at how algorithms create relations or interrelations between culture, people and technology.

Online service providers (OSPs) such as Facebook, Google, Microsoft and Twitter are significantly shaping the informational environment and influencing user’s experiences and interactions with their public role as *information gatekeepers* (Taddeo & Floridi, 2016, p. 1577; Calhoun, 2002). And Striphas claims that personalization and the recommendation algorithms that are used by OSPs such as Google, Facebook, Twitter, Netflix and etc. change “how the category of culture has long been practiced, experienced and understood” (Striphas, 2015, p. 395).

Therefore, it is believed that it will be essential to understand how algorithms and culture are related, what kind of interrelations occur between the field of culture and technology, how the field and discourse of culture is influenced in the sphere of algorithmic culture and how cultural studies become a part of the discussions surrounding algorithms.

1.1.7. What is the Relation of Algorithms to Culture and Cultural Studies?

It is believed that this question can be answered with another question. Hallinan & Striphas ask if there is any difference between a human being’s determining and a computer system’s determining and selecting movies, news, information “tailored to individual’s taste preferences” (Hallinan & Striphas, 2016, p. 118-119). Personalization and recommending algorithms offer users *relevant* media and information consumption which are based on their previous preferences and also on other *similar* people’s likes and preferences. Therefore, these algorithms are playing an important and a critical role “in deciding which articles (or parts thereof) gain admission to the cultural realm, and in what form” (ibid, p. 129).

And it cannot be denied that personalization and recommending systems are creating a kind of ease and satisfaction for the users, enabling them to find more *relevant* information they seek and more *sophisticated* and *similar* content they search. However, “-theoretically- it is resulting in a closed commercial loop in which culture conforms to, more than it confronts its users” (ibid, p. 122).

As algorithms become more decisive, online service providers are fast becoming “the new apostles of culture” (Striphas, 2015, p. 407). Considering the trending algorithms, algorithm is “preferring novelty in public discourse over phenomena with a longer shelf-life” and in turn this makes “public more attuned to the ‘new’ and viral memes more than slow building discussions and topics" (Gillespie, 2012). Therefore, it can be concluded that algorithms and online service providers are taking active role in shaping the cultural heritage.

Algorithms have been lately a discussion of Cultural Studies, too. Daniel Neyland, in his article, criticizes the trend which has the tendency to consider algorithms as mechanisms which are "likely to change our lives, beyond our control, inaccessible, working independently and incomprehensible" and calls this situation as "an alluring and compelling drama" (Neyland, 2016, p. 51). He further continues (ibid):

> We are told that algorithms trap us and control our lives (Spring 2011), produce new ways to undermine our privacy (Stalder and Mayer 2009) and ''algorithms have the capacity to shape social and cultural formations and impact directly on individual lives,'' (Beer 2009: 994), that ''power is increasingly in the algorithm,'' (Lash 2007: 71), and that algorithms ''acquire the status of truth . . . They become real.'' (Slavin 2011: n.p.).

Although Neyland's criticism is strong and sharp, there is one important issue that he addresses; and it is the *agency* of the user or audience which has been an everlasting and major discussion of the Cultural Studies. Similarly, Jonathan Cohn criticizes that scholarship of algorithmic culture "tends to present algorithms as opaque, static, and despotic, it also presents users as incapable of critical reflection, transgressive actions, or the simple act of decoding that has been a central facet of Cultural Studies since beginning" (Cohn, 2016, p. 678). As being against seeing the digital technologies as saviors, he also criticizes underestimating the *agency* of the users in understanding, reading and decoding the culture surrounding them, suggesting that users or audiences are not powerless (ibid).

Therefore, as being aware of the critics related to Cultural Studies' view on the discussion, this thesis study adopts Mike Ananny's term *networked information algorithms* (NIA) which does not regard the "algorithmic system just as code and data, but as an assemblage of human and non-human actors" (Ananny & Crawford, 2016, p. 11). They are "of institutionally situated code, practices, and norms with the power to create, sustain, and signify relationships among people and data through minimally observable semiautonomous action" (Ananny, 2016, p. 93). He develops and uses this term for two main reasons: to distinguish the research object "from computer science's purely mathematical, mechanistic focus, and to consider the *ethics*[5] of the sociotechnical *relationships* producing, interpreting and relying upon the formation processed by computational algorithms" (Ananny, 2016, p. 97).

As Gillespie puts it, a sociological analysis should not understand algorithms as "abstract, technical achievements, but must unpack the warm human and institutional choices that lie behind these cold mechanisms" (Gillespie, 2014, p. 169). That is to say, algorithms and algorithmic system are not just what designers create or what algorithms make of the information they process, but they are also what users make of them, constantly (ibid, p. 187). This means that algorithmic systems are human – algorithm assemblage and socio – technical assemblages, "joining together the human, nonhuman, the cultural and the computational" (Striphas, 2015, p. 408). That is to say, the way algorithms operate does not function in the way it is programmed, but it learns from the data, the data that people provide to the system. The way people interact with the algorithms and the data they continue to produce create a socio – technical assemblage where both human and machine inputs are actively contributing to algorithmic culture.

Having discussed the terms and questions surrounding the algorithmic culture, this thesis study will now focus and expand on concepts and phenomenon that come along with it. It is believed that algorithmic culture is affecting and causing major changes in the socio-technological field which are categorized under the titles of *information diet, economy politics of algorithms* and *surveillance.*

1.2. INFORMATION DIET

What this thesis calls as information diet is the *personalization* of the web, search results, news feed and information consumption; *filter bubbles* and *echo chambers.* It is believed that algorithms operating on the web and on online service providers' platforms are creating an *appetite* for information consumption, thus creating new *realities* for users. What will be scrutinized in this chapter is the *invisible* algorithmic editing of the web and their gate-keeping function which is all together believed to be causing an *informational determinism.*

---

[5] Emphasis is added.

1.2.1. Personalization

Personalized search for everyone[6]

On the web, users are producing and being exposed to information more than ever before, and it can be hard to find one's way through these huge amounts of information. Therefore, online service providers introduced their users with *personalization features* in order to deal with the emerging situation. These personalization features are "algorithms that tailor information based on what the user needs, wants and who s/he[7] knows on the social web" (Bozdağ, 2013, p. 209).

Personalization is an important strategy for many top web sites and platforms. It is because this algorithmic selection is giving those platforms kind of governance which is "automated, instantaneous (real time), predominantly based on big data, partially self-learning, and always context-related/personalized, applying customized selection criteria" (Just & Latzer, 2017, p. 247).

This personalization happens "on the basis of one's user characteristics (socio-demographics) and own (previous) user behavior, others' (previous) user behavior, information on user-connectedness, and location" (ibid, p. 247-248). The database that is to be used for the personalization can be consisting of both active user input and user's passive data. While an active input of the user can be a feedback, passive data can be location, social contacts and clicks (ibid, p. 248). Engin Bozdağ suggests that most of the personalization systems are based on some kind of user profiles, which may include demographic information such as, name, age, country; and it can also include the interests, tastes and preferences of a user or a group (2013, p. 213). He explains that the aim of this user profiling is "to collect information about the subjects in which a user is interested, and the length of time over which they have exhibited this interest, in order to improve the quality of information access and infer the user's intentions" (ibid).

[6] Google has posted on their official blog an article titled p*ersonalized search for everyone* on 4 December 2009 by Bryan Horling and Matthew Kulick, explaining people how their searches and results are personalized (Horling & Kulick, 2009).

[7] The indication is added.

Borrowing the Bozdağ's adaptation, Figure 1 is showing how personalization based on user profile happens.

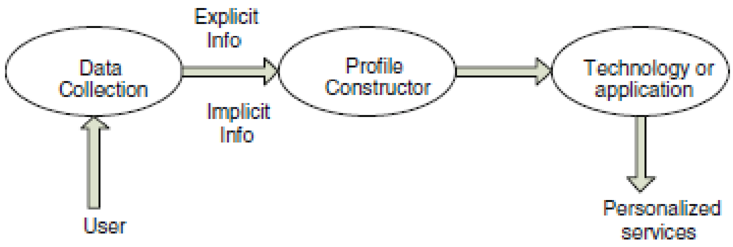


Figure 1: Personalization based on user profile (Bozdağ, 2013, p. 213)[8].

He explains that first of all, data and information is collected from the user. Depending on the collection process type, explicit or implicit data can be extracted. In the second part, collected data and information is analyzed and processed. In the final part, "compiled user profile is used in actual web services" (ibid). What he means with 'explicit or implicit building of user profile' is that if "user customizes the information source herself/himself[9] … before the personalization starts", then it is an explicit building of the profile, but if the system decides what the user pays attention to via different factors such as "web usage mining (i.e., previous interaction with the systems such as clickthroughs, browsing history, previous queries…), IP address, cookies", then it is the implicit building of the user profile (ibid).

Although personalization filters help users to find the information they want to know, hear and see among many other irrelevant information on the web (Pariser, 2011a, p. 11), and although Goldman (2006) discusses that "personalization algorithms increase relevancy… diminish the weight given to popularity-based metrics… reduces the structural biases due to popularity… (by producing) a different output per individual user", it is believed this design is also introducing new problems, too (as cited in Bozdağ, 2015, p.25).

[8] Bozdağ adapts this figure from the work of Gauch, Speretta, Chandramouli and Micarelli (2007).

[9] The indication is added.

First of all, when people are exposed to content that is more similar to their preferences and search histories; it is believed that this situation is increasing the individualization in societies, creating fragmentation, causing less unplanned encounters and less shared experiences. And in turn, this is decreasing social cohesion and increasing a sense of control on individuals, causing less privacy and freedom (Just and Latzer, 2017, p. 254). However, Sunstein (2001, p.131) suggests that it is also very important to have "unanticipated, unchosen exposures and shared experiences" (as cited in Taddeo & Floridi, 2016, p. 1582).

On the other hand, it is thought that it is very challenging for users to quit their personalization filters, because the home pages of the platforms like YouTube, Facebook, Twitter makes them feels like *home*, enabling them to see things they enjoy reading, listening and watching. However, custom-tailoring of the search results are not only threatening the diversity of the information sources, it is also "undermining the possibilities of sharing cultural background and experiences and reduces chances of being exposed to sources, opinions and information that may support or convey different world views" (Taddeo & Floridi, 2016, p. 1581-1582).

1.2.2. Filter Bubbles

Online service providers such Facebook, Twitter and Google are playing an important role in user's connectedness and in providing information. They are more powerful than the *traditional* media outlets, because they are addressing such a huge audience which any other traditional media outlets could not have reached. And increasingly, they have become the most prominent news source for many people, -especially in some parts of the world, they are used as the only source of information.

When personalization algorithms operate on the platforms that people get information, it effects how people understand and perceive the world. Therefore, personalization algorithms are becoming phenomenon that affects, shape and alter people's world views. According to Eli Pariser, two users get different results for the same query, because new services, search results and also social networks are tailored in accordance with the preferences of the users. Therefore, what is newsworthy for one person may not have the same importance or relevance for another person (Pariser, 2011b). However, when information services are personalized this much, “the diversity of knowledge and political dialogue may be undermined” and “we are led… into filter bubbles where we find only the news we expect and the political perspectives we already hold dear” (as cited in Gillespie, 2014, p. 188).

Pariser suggests that filter bubbles on the social networks eliminates the posts of the friends who are not sharing the same ideas with the user. And this causes the narrowing of the world view, because people cannot encounter with the opinions that can challenge their point of views (2011b). Engin Bozdağ suggests that “this might create a monoculture where user can get trapped in their *filter bubbles*” (Bozdağ, 2013, p. 209). In *real* world, or in social psychology tradition, it is also clear that people tend to come together, communicate, build relationships and share experiences with people that are similar to themselves, their habits of thought and lifestyles. However, this thesis study claims that in *real* world experiences, individuals have the opportunities to come across with people holding challenging and different world views. And personalization algorithms are closed to change by blocking and eliminating the opposing ideas *automatically*.

Thus, personalization of the web and social networks and the filters operating on these platforms are creating *algorithmic gatekeeping* which is creating different *realities* for different users. Therefore, online service providers’ platforms, where the information flows are becoming the new gatekeepers of the society, are algorithmically editing what is to be omitted, included, filtered and eliminated. Metoyer-Duran (1993) describes that there are two conditions for an agent to be a gatekeeper;

> if the agent is controlling access to information and acting as an inhibitor by limiting and restricting the scope of information, and if the agent is acting as an innovator, communication channel, link, intermediary, helper, adapter, opinion leader, breaker and facilitator (as cited in Taddeo & Floridi, 2016, p. 1583).

The first one is about the moral responsibilities of the service providers, while the second condition is revealing the initiative role of the gatekeepers. Therefore, it is important to realize that online service providers –especially search engines and social networks- are becoming like publishers which are not filtering in line with the *ruling* *power* of the state or media bosses[10], but in line with the user's preferences and tastes (ibid, p. 1579). Therefore, these algorithmic editing of the news and the web is believed to be creating different realities which affects user's information diet and world views. That is to say, algorithmic selection, editing or gatekeeping contributes to reality construction which is actually a way of governance accompanied by selection or elimination of the information. And so, *algorithmically formed reality* starts governing behavior, action and many other choices in daily life (Just and Latzer, 2017, p. 247).

Furthermore, algorithmic selection and gatekeeping has similar and different features compared to traditional media gatekeeping and their news selection. Just like in traditional media, algorithmic gatekeeping[11] uses *agenda-setting* and *framing*, too. Algorithmic electing / editing affects what users think, which is similar to agenda-setting; and also, it affects how they think, which is similar to framing. And in the end, it affects how people behave and act (Just and Latzer, 2017, p. 245). There are also some differences in reality construction between traditional media and algorithmic selection. A big difference is "the *personalization*[12] of reality construction that contributes to further individualization in societies, and the *constellation* of actors that are constituent part of the Internet's ecosystem" (ibid, p. 247).

As a result, the filter bubble which "is your own personal, unique universe of information that you live online" cause problems in return of *relevancy* (Pariser, 2011b). As Pariser argues (2011a), due to personalization algorithms, "online services can cause citizens to be ill-informed about current events and may have increasingly idiosyncratic perceptions about the importance or current events and political issues" (as

---

[10] However, this study is also aware of the fact that even though it is not the bosses of the social networks who control, edit news and decide which news to be published and get through, it is their algorithms which are decision-making. And this is still making them responsible and accountable.

[11]Gatekeeping is defined as "the process of culling and crafting countless bits of information into the limited number of messages that reach people each day, and it is the center of the media's role in modern public life" (Shoemaker & Vos, 2009, p. 1). And "this process determines not only which information is selected, but also what the content and nature of messages, such as news, will be" (ibid). As a result, *algorithmic gatekeeping* is used to describe the process of algorithms to decide, omit and edit information on the Internet and social networks. It addresses the ability of automated algorithms to select which information to be at the top of individuals' newsfeeds or search results. It addresses the autonomous and decision-making characteristics of the algorithms with regard to delivery of information.

[12] The italic emphasis on the words *personalization* and *constellation* is added.

cited in Bozdağ, 2013, p. 218). As people cannot see which information or posts are omitted from their social networks and they are subject to more similar ideas and posts, it is believed that this situation leading to creation of homophily[13] on social networks.

Pariser suggests that with these algorithms, “instead of a balanced information diet, users can end up surrounded by junk food” (Pariser, 2011b). Filter bubbles are diminishing the information diversity and threatening pluralistic democratic structure of web by showing different results to two different users for the same query. Therefore, it is kind of breaking the shared social reality structure which is a detrimental effect on democracy (Just and Letzer, 2017, p. 246).

Pariser claims that living in filter bubbles is like losing the synapsis of the neurons in the brain. This means that there is information accumulated in the brain or in the web and in social networks, but they cannot communicate with each other. He thinks that with this loss of connection, “we may be giving ourselves a kind of global lobotomy” (Pariser, 2011a, p. 19). He also develops another criticism and claims that in filter bubbles, people are making a lot of *bonding capital*, but very less *bridging capital*.[14] He says that our virtual and real neighbors are getting to look more like us. That is to say, we are getting a lot of bonding, but not many bridging capitals. However, “it is the

[13] McPherson, Lovin and Cook defines homophily in their article “Birds of a Feather: Homophily in Social Networks” as the principle that “structures network ties of every type… The result is that people’s personal networks are homogeneous with regard to many sociodemographic, behavioral, and intrapersonal characteristics” and it “limits people’s social worlds” and result in “powerful implications for the information people receive, the attitudes they form, and the interactions they experience” (McPherson, Lovin & Cook, 2001, p. 415). It is believed that ‘homophily’ happens in two ways: Not only on social networks, but also in the ‘actual world’, people tend to like, share and be part of the things they are interested in. They surround themselves with ideas similar to that of themselves. However, this homogenization of life traps people into circles where they do not come across with counter ideas and point of views. Secondly, this is also happening on the social networks with algorithms which recommend similar contents and omit counter information and ideas from newsfeeds. It is believed that this situation is creating homophily on the Internet, people are deprived of information or posts that they are not familiar with. It is important, because this narrows people’s world views. And the difference between the homophily on the social networks and the actual world is that people do come across with counter ideas in the actual world. However, on social networks, the decision-making process is given to algorithms which automate omission of the counter ideas and recommendation of the similar contents. That is to say, in the actual world, people are aware of the counter ideas, but with the automated algorithms, people are not even aware that there is a counter point of view, because it is already omitted without the awareness of the individual.

[14] In his book *Bowling Alone* (2000), Robert Putnam identifies two types of social capital; bonding and bridging capital.

bridging [capital] that creates our sense of 'public' – the space where we address the problems that transcend our niches and narrow self-interests" (ibid, p. 17).

As a result, it needs to be made sure that online service providers are upholding the plurality, democracy on the social networks and on the web. Online gatekeepers (algorithms or OSPs) should uphold the public interest. In a world which is curated by algorithms, users need to be sure that they are also being exposed to uncomfortable and challenging ideas, too (Pariser, 2011b). It is needed that "these algorithms have encoded in them a sense of the public life, a sense of civic responsibility" and they are transparent enough to see rules determining what gets through the filters, and people also need to be empowered by giving them some control to decide what gets through and not (ibid).

1.2.3. Echo Chambers

Can we really follow what is happening around the world and in Turkey with hashtags and newsfeeds? How does a reaction that we show for any phenomena with social media applications change social, political, cultural and economic fields[15] (Binark, 2017, p. 19)? These are believed to be important questions which open up the discussions around *echo chambers.*

Personalization filters which are causing filter bubbles, also causing echo chambers. For some, echo chamber is another way of saying filter bubbles and they are similar to each other in design and working. Echo chamber occurs when "information, ideas, or beliefs are repeatedly pushed in an enclosed system like mind, newsfeed or social circle, while other views are prohibited" (Minute Videos, 2016).

Personalization algorithm automatically eliminates posts of the users who are not sharing the same ideas, likes and viewpoints. This means that there is not enough space for encounters which results in learning or which can develop insight. This situation can affect how a person perceives the world, events and discussions surrounding her/him. And as Newell and Marabelli (2015) discussed, "filtering algorithms that create 'echo

[15] Translation belongs to me.

chambers' devoid of contradictory information may impede decisional autonomy" (Mittelstadt et al., 2016, p. 9). Echo chambers in social networks are being discussed more with the political discourse such as the role and effect of social networks in creating and trapping users in echo chambers during elections[16].

Sunstein (2007) argued that "availability of manual filters on the Internet and the option to communicate only with like-minded others, group polarization will arise and people will end in more extreme positions" (as cited in Bozdağ, 2015, p. 6). Sunstein used the term "echo chambers" to indicate this group polarization (ibid). However, the term has undergone a shift in meaning. It does not only "encompasses opaque automatic cyberbalkanization[17] imposed on users by the algorithms of the online platforms as emphasized by Pariser, it also includes other non-automatic voluntary selective exposure and biased information seeking and group polarization" (ibid).

As a result, echo chambers are causing and contributing to group polarization in social networks, homophily, isolation, information deprivation and post-truth.[18] In order not to cut people and different voices out of social networks over politics, one solution can be interacting more and more with people who have different opinions on social media.

[16] In relation to this, a recent decision of Facebook on how to regulate newsfeed can be given as an example. After being accused of circulating and enabling fake news on users' newsfeeds, Facebook was criticized for distorting the reality of the users as each of them was entrapped in their own realities and news that appeal to them. As a result of this, Facebook announced their decision about their prioritizing algorithms that post of friends or families will be more prioritized over public content in the name of bringing people closer. However, it is believed that the real reason behind this act is that they do not want to be related to fake news problems anymore, they got tired of being scapegoated for the fake news in relation to USA elections. Therefore, this can be read as their way of getting rid of the problem by prioritizing posts of family and friends over content related to public discourse and discussions (Mosseri, 2018).

[17]Cyberbalkanization means segregation and separation of the Internet structure into groups where everybody shares the same interests, leading to closed and narrow-minded behavior to opposing opinions. That is to say, 'balkanization' means "the degree to which resources exist as disconnected islands within a larger population" (Alstyne & Brynjolfsson, 1997, p. 6). However, the thesis suggests that we need to find another term for the segregation of the Internet instead of cyberbalkanization. This appropriation can create sensitivity for the people of Balkans. And it is considered as a labelling association.

[18] Post-truth is described by Oxford Dictionaries as the year of the word and it means "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief" (Post-truth, n.d.). However, the term was first used by Steve Tesich in 1992 in his essay about Iran-Contra scandal and Persian Gulf war in magazine "The Nation", he described the politics of post-truth as "we, as a free people, have freely decided that we want to live in some post-truth world" (Flood, 2016).

1.3. ECONOMY POLITICS OF ALGORITHMS

"*If you are not paying for something, you are not a customer; you're the product being sold*" (Lewis, 2010).

What this study calls as economy politics of algorithms is the *platformization* and *dominance* of online service providers (OSPs) due to their opaque nature; *targeted ads* emerging from analytics of the aggregated data to better sell the products not for groups, but for individuals and optimizing systems which are based on personalization algorithms and profiling of the users; *behavior market* which is based on emotion economies and recommending algorithms. Questioning the ownership of the data, it is believed that value laden data which have become the new currency are creating virtual monopolies in the web and social networks. And in return, these platforms are becoming the new canals where capitalism flows and acts.

Before discussing the *platformization* and *dominance* of OSPs, *behavior market*, *targeted ads,* it is important to discuss why and how data are value laden, how data becomes a part of the economy and why data are important for the market.

Users as being highly networked individuals are producing –consciously or unconsciously- data about themselves with networked digital devices through various applications. Every act on the digital realm is leaving data trails behind which are collected, tracked, evaluated, monetized and surveilled for economic and security reasons. According to Adrejevic and Burdon (2015), people are now living in a media structure where they produce "a continuous stream of expression and information about their identities, movements and interactions" (as cited in Carah, 2017 p. 390). And the data related to every aspect of daily life are collected passively which means that they are collected without active involvement of the user or without their knowledge with the techniques such as cookies, web bugs and observation of online communities and individuals (ESOMAR, 2009, p. 3). However, it is believed that the automated and passive collection of data "passive-izes" the user interactivity resulting in the fact that users are generating data more than they participate (Andrejevic & Burdon, 2015, p. 20). And in the business world, the collected data are put into use with various techniques and regarded as a valuable economic source which is currently described as new oil, gold mine or the new currency (ibid).

Data are value laden, because they provide enormous information about the user's demographics, habits, choices, ideas and way of living. Data are able to tell about preferences of a certain user. According to Greg Elmer (2004, p. 9), this is *consumer profiling* which is described as "an ongoing distribution and cataloguing of information about desires, habits, and location of individuals and groups" by OSPs (as cited in Mager, 2012, p. 772). The profiling is conducted based on clicks, search terms, search history and locations of the users. Hence, user's preferences and profiles start to have economic value by selling them to advertising clients (ibid). And in return, users are exposed to advertisements tailored to their preferences, tastes and needs. In this sense, data are valuable, because advertisers have the opportunity to know *exactly* who their customers are and what they are specifically looking for. In this respect, data are described as goldmine, new oil or new currency, because "it enables search engines to relate advertisements to user's interests and desires" and as a result, the value is not lying on the algorithms, but on the databases and consumer data (ibid, p. 776). The more users engage with mobile devices, the more databases are produced which algorithms will operate on and the more user data will be sold to advertisement clients and the more users will be exposed to tailored advertisements.

Data that are collected and sold to clients as a commodity by OPSs become a part of the economy. Christian Fuchs (2011) provides a figure in explaining how Google's –one of the leading platforms in exploiting user data- capital accumulation process works.

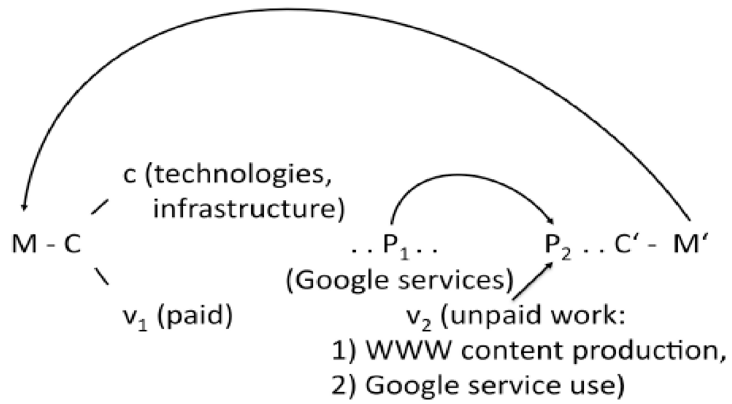


Figure 2: Google's capital accumulation process (Fuchs, 2011).

According to Fuchs, Google is investing money (M) to buy capital (C) such as technological infrastructure (including servers, computers etc.) and labor power (v1) which means paid Google employees. Paid employees are working at Google to produce (P1) Google services such as Google Search, YouTube, Gmail and etc. (Fuchs, 2011). In this point, it is important to realize that these “Google services are no commodities, they are not sold to users, but rather provided to users without payment” (ibid). Unpaid labor of content creators (v2) engage in different activities on the web such as searching, e-mailing, blogging, uploading videos and pictures, reading, watching and etc. (P2) (ibid). As a result, unpaid work of Google users and www content creators are creating a new commodity (C’) which is called “Google prosumer commodity”, and this prosumer commodity is sold to advertising clients which is shown as C’ – M’ process in the figure (ibid). This means that Google is getting money (M’) from advertisers and they can use the prosumer commodity to target advertisement to Google users, and in this way, Google is increasing its invested money by making profit of the user data (ibid). However, Google is not the only one who is doing this, many leading OSPs such as Facebook, Twitter and etc. are commodifying, exploiting the user data by selling the unpaid work of the users to advertisers. Therefore, the capital accumulation process given in the table can be applied to other platforms which exploit users and user data.

As a result, data have become an important value for the market, because people put their personal information regarding their daily lives, identities, tastes and preferences into data bases with new media devices. These narrative data are sold to advertisers and third parties, and in return, this creates “an open-ended and responsive form of” advertising which means that “the more users engage with” online services and provide data, the more advertisers “are able to use algorithms to attune themselves to cultural lives and online flows” of people (Carah, 2017, p. 387). It is important to notice that advertisers’ capacity to respond culture of people stems from the capacity to use data-driven content, not from their capacity to make sense of the characteristics that people attribute to culture (ibid). Data are valuable for the market, because they provide *real world interaction* with the users which helps advertisers to target products to audiences more accurately. Algorithmic data enable not only targeting, evaluation and advertising, but it also enables audiences to be calculated (ibid, p.397). The power of third parties to calculate, evaluate and integrate users into their products makes data an important value for the market. Thus, commodification of the user data is creating new canals where marketers and capitalism can act and flow.

When this is the case, it is also important to understand the neoliberal ethos and changing values of the society in order to better comprehend why people are not caring enough about how their personal data are used (unethically) by third parties, how they make use of data, how data become a part of commodification and how they join in the flow. Even though users know about commodification, monetization or dataveillance over their data, they continue to use services, applications or platforms. This is believed to be closely related to the changing values of the society with new Information and Communications Technologies (ICT) which brought new needs.

Firstly, we can talk about three groups in the society: the first one which is aware of commodification of data, but cannot help using: the second one which is not aware of the situation: the third one which is aware, but does not care. The *first* group may still continue using services, because they cannot give up digital pleasure of communicating, sharing and expressing. Concerns such as being popular, visible or recognized are also other drives that lead them to use and to perform on social networks and the Internet. Users would also like to keep up with the flow on social networks in order not to feel left behind. Also, these applications are designed to keep users active, to share, to comment, to perform, to give attention and time. It is possible to say that it is not quite likely to disconnect or to stay out of digital devices which collect and monetize data, because business model of many corporations/individuals depends on ICTs. Also, these technologies are active at different realms of human life ranging from banking, shopping, communicating, entertaining, studying, researching and etc. Thus, if one disconnects, it means that one person not only loses connection with the flow of social media, but also with the main activities of life. Considering the *second* group who is not aware, it is interesting to think about how people as being users/citizens trust companies or governments about the information they provide. People tend to think they have nothing to hide from government and they are not concerned about governments' efforts on making citizens transparent. Another thing is that they question 'what is the possible importance of my mundane data', emphasizing that s/he is an ordinary person. However, data have economic value regardless of the importance attributed by people. It is possible to say that this situation stems from the fact that they lack of critical media literacy. Regarding the *third* group who does not care, there can be different motives. The first one can be that users may think they are benefitting from the free service policy of the platforms. They may think that by commodification of their data, they access to platforms which provide them entertainment, information, communication and etc. Thus, they are aware that their data are abused, but in return, they are accessing 'free' content on the web, making use of 'free' services and receiving discounts. In this way, this situation is considered as 'win win' by many users. It is also possible to think that these platforms are making a promise by saying that 'I will provide you a better consumption experience'. It is not only in the sense of receiving targeted ads on products, but also it is about consumption of knowledge, art, music and etc. on platforms and applications. In this way, time is saved, as people do not have to look for the content they need. That is to say, users are granted a level of easiness, when they want to use the platforms.

Thus, even though users are (partly) aware of the affective, immaterial and free labor structure of the Internet and exploitation on the networks, they give up their claim over their data. They even become the foundation of the capitalist system with its prosumer structure. As a result, it will not be wrong to say that users are producing data -contributing to systems- *voluntarily*. There is a voluntary labor on social networks where labor and capital are intertwined. And, this is considered as the first change in the neoliberal system. In relation to this, it is important to discuss that people are on these platforms, producing 7/24 data about their status, actions and carrying offline world into online, because the system is designed for this. As Ergin Bulut discusses, "the fact that constant connectivity of the consumers, liking and sharing something and producing content on digital platforms is very important for neoliberal capitalism to reproduce itself" (2016, p. 21)[19]. With the development on ICTs, the phenomenon of *constant connectivity* and *constant sharing* is considered as the second change. Thus, when user participation constitutes the business structure of the platforms and when users

[19] Translation belongs to me.

participate 7/24, we can talk about *the blurring lines* between work and free time (ibid). It is a blurring line, because users are not paid for their productions and this creates free labor. And, this is considered as the third change. As a result of this, as Bulut discusses labor becomes a structure where we put everything about ourselves beyond physical and intellectual effort (ibid, p. 23), because we try to perform our unique subjectivity. Thus, everything -every part of our lives from sleeping to researching- can be understood as a commodity. And, this is considered as the fourth change. By this way, data about our lives becomes the final product and as being users, we give up our rights over the product that we produce to companies with user agreements, when we accept the user terms and conditions before we use the platforms and this clearly shows that we are alienated from our labor (ibid, p. 27). And, this alienation is considered as the fifth change.

1.3.1. Platformization and Dominance of OSPs

Let us begin with a hypothesis. You have a social media account which enables you to connect, share and communicate with friends, but you did not pay anything for the service you get. You use different kinds of search engines which enable you to get information, search and learn, but you did not pay in return. You use web and services to blog, create content and e-mail, but you paid nothing. Then, one question which needs to be asked is that; how can a service be *free* in a capitalistic society?

Or let us think from this perspective. It was announced on October 2006 that Google purchased YouTube "for stock that it valued at $1.65 billion" (Sorkin & Peters, 2006). Another example can be Facebook. It purchased Instagram for $1 billion in 2012 and it also purchased WhatsApp for $19 billion in 2014 (Page, 2015). Then, a person must question, if these companies do not demand money from their users for their services, how can they earn money and how can these companies have such great amount of monetary value? That is to say, if WhatsApp is free of charge, how can it have a value of $19 billion?

Then, it should be asked; is the *free service* policy of the social media platforms and web services an illusion to capture more users to gain more profit from them? And if the answer is yes, then how is it possible? The answer is actually quite simple. "Users are getting service for free, while ‘paying’ with their data” (Mager, 2012, p. 772). Free use of these services and platforms allure people to participate, create content and get pleasure of communicating. However, the truth is that very few users are aware of the fact that their personal data are commodified and they become the product that is sold. And also, very few users consider this situation as problematic without questioning the ownership of the data and monetary importance of their own data. The data users give away can be demographic and geographic data and also can include lifestyle data. It means that the variety of the data can range from users’ name, age, gender, education and location to habits, tastes, preferences, fears and tendencies. This ignorance is also achieved by the closed and spy-like operations of the platforms which make it harder for users to understand the economic logic (ibid, p. 777). Another point is that default settings of the social media platforms and search engines are programmed to collect data, not to protect users’ privacy. Therefore, it is believed that the free usage of these platforms results in two main things; commodification of data and exploitation of the user (data). Users are exploited, because their data are sold to advertisers and also their user-generated content is creating a surplus value, as they continue to produce and use the services of these platforms. This labor can be turned into surplus value by using these services such as writing an e-mail, using maps, watching a video, searching a subject, translating a text or reading, and also by active participation such as writing a blog, uploading a video, commenting on a subject, sharing an image. These activities are called “Internet prosumer commodity” (Fuchs, 2011), because they constitute unpaid labor of the prosumers. Therefore, using these platforms and working for those platforms “means being permanently exploited and dispossessed of the profit that is being created by the users and employees” (ibid).

Even though these platforms have the nature of democratizing by enabling user-generated content, there is a discursive work lying on the word *platform* which implies different meanings attributed to it. As Tarleton Gillespie suggests the term platform is deployed sometimes “as technical ‘platforms’, sometimes as ‘platforms’ from which to speak, sometimes as ‘platforms’ of opportunity” (Gillespie, 2010, p. 347). The term platform helps these service providers to stage their position and to reveal the situation specific to their services which stand: “between user-generated and commercially-produced content, between cultivating community and serving up advertising, between intervening in the delivery of content and remaining neutral" (ibid, p. 348). There is a semantic richness in the selection of the word platform. They are not only technical bases where codes are run, but also, they are bases to communicate, interact and *sell* (ibid, p. 351). In contrast to traditional media, these platforms enable users to speak and to be heard. They also increase users' social capital. However, these platforms are changing from being neutral, open and progressive to something more commercial, as they are funded by advertisers. Therefore, it is a monetized platform which offers commercial opportunities for advertisers to find their customers.

The business model of many Internet companies such as Google, Facebook, Amazon or Twitter leading to *platformization* which means that these companies have market more than one side and serve more than one or two customers which are also interdependent to each other (Just & Latzer, 2017 p. 251). As being market-makers, they become active intermediaries between two demand sides, focusing on the relationship and interdependencies between the platforms and the media players (ibid). That is to say, they have the power to control the access to their services, other services and also the products (ibid). Therefore, it becomes a monopolistic structure which regulates the relationships and controls the access to products and services. Also, these platforms are "a cultural intermediary" where they curate culture, information and life (Gillespie, 2010, p. 353). Applying algorithmic selection on their platforms, they do not only control or intermediate the markets, but also culture.

It is believed that platformization is leading to *dominance* of these corporations. As these platforms become more *ubiquitous* in life, the more dominant they get in the cultural field. It is because they do not only have the services which people use to socialize, work, shop or get informed, but also they shape *how* you perform these actions such as "how you search, organize and perceive in contexts like the workplace, private life, culture, politics, household, shopping, consumption, entertainment and sport etc." (Fuchs, 2011). The word "to google" is a good example of dominance of the platforms. It means "search for information about (someone or something) on the Internet using the search engine Google" (Google, n.d.). This situation reveals that "the products of large monopoly capitalist companies have become so present in capitalist society" that it is used to expresses the enormous usage of these services and products (Fuchs, 2011).

Moreover, these platforms dominate the market by the multitude of their services. For example, considering the multitude of Google services, it includes "Google Search, Google Mail, Google Maps, Google Earth, Google Analytics… Google +, and its share… in the Android" provides data about the users (Mager, 2012, p. 772). Therefore, it can be concluded that Google has created its own monopoly by dominating the market with the multitude of its services and products.

These platforms dominate the market also by acquiring the talents or other companies that become prominent. It is because these big companies "are being challenged by small, groundbreaking companies that could maneuver much faster than a major corporation" (Weber, 2011). Being aware of the potential of startups, big corporations acquire talents which are promising and, in this way, they contribute to their own capital structure. Facebook, for instance, bought the social media platform FriendFeed in 2009, Instagram in 2012, WhatsApp in 2014 and a virtual reality company Oculus VR in 2014 (Betters, 2014). On Facebook's acquiring strategy, co-founder of Facebook Mark Zuckerberg stated that

> "We have not once bought a company for the company. We buy companies to get excellent people… In order to have a really entrepreneurial culture one of the key things is to make sure we're recruiting the best people. One of the ways to do this is to focus on acquiring great companies with great founders" (Miglo, 2016, p. 216).

In this way, companies are increasing their share and value in the market and contribute to their dominance among their competitors. Even though Zuckerberg says he focuses on a shared vision, he admitted that he scares small startups to convince them for cooperation. He states that "… but I think if you are trying to help convince people that they want to join you, helping them understand all the pain that they would have to go through to build it out independently is a valuable tactic" (Heath, 2017).

Another example how these platforms dominate the market is related to their strategy of signing up to websites with social network accounts such as Facebook, Google etc. When a user wants to sign up to a website, they are also offered to sign in with their social network accounts which may seem like an easier option for the users. In this way, users do not have to remember different password for different websites and it becomes more manageable for them. However, one thing is at risk. Those third-party websites will be automatically able to access personal information such as contacts or friends and they may also be able to post comments on behalf of the users, if users do not read carefully for what they are giving authorization permission. If a user continues with the default settings when signing up for a website via Facebook or Google, third party websites will demand more authorization than they actually need. One example can be academia.edu. When a user wants to sign up for the platform, it gives three options to users; they either need to sign up with her/his Facebook account, Google account or with e-mail address. And if the users continue with the default settings of signing up with the Facebook, then they are giving too much information such as lists of their friends on Facebook and her/his personal e-mail address. This shows that the monopoly of the companies can be integrated into different needs ranging from socializing, entertaining, and communicating to learning. Therefore, it can be concluded that big companies are dominating the market also with their interdependencies and relationships with the third parties.

1.3.2. Targeted Ads[20]

When a person looks for information on search engines – most probably using Google-, types the keyword on the search box and browses through pages, blogs and websites, s/he will not only get the informative articles or papers, but also commercial links and ads. That is to say, if a person search for the word "vegan", then it is likely that s/he will get suggestions for vegan restaurants nearby based on her/his location and in the language of that particular location. Also, connected to her/his personal interests, s/he will get different ads about vegan products or commercial suggestions about being vegan in general. These commercials will continue to haunt through the web, as s/he continues to visit web pages and blogs. Therefore, the companies are creating a value from the need of information and the "need for information is being transferred into a customer desire" which "Google tries to satisfy by showing… commercials related to

[20] This title and the narrative story in the beginning are inspired by the Astrid Mager's article *Algorithmic Ideology* published in 2012.

(her/his) own search", and it is because the search engine technology is tightly entangled with capitalist society (Mager, 2012, p. 770).

Moreover, if a person checks the URL (https://www.google.com/ads/preferences/), s/he will see her/his own interests and preferences collected by cookies and which are used for targeted advertising (Fuchs, 2011). This means that a person can see what Google thought that s/he has been interested in lately. They put a keyword for each letter of the alphabet displaying current interests and searches. So, for example, at the time of writing this thesis, Google correctly identified these personal interests as being "yoga & Pilates", "blues", "cats" and "running & hiking". This means that they know you and target you. And this knowledge of current interests is commodified for business. Regarding this, there are questions that need to be addressed. How does targeted advertising happen? How does it affect? And also, what are the causes?

It is no secret that online advertising and digital advertising constitute the big part of the economy on the Internet. It is the main economic driver which funds many websites, services and even the platforms itself (Guha, Cheng & Francis, 2010, p. 81). What is taking place on the Internet is a business model based on advertising. Traditional ways of advertising such as newspapers, radio and billboards are changed with online ads which results in targeted advertising. Targeting happens "by gathering a great deal of user information… search histories, web browsing behaviors, online social networking profiles, and mobile locations" and it can also be a user's demographics such as gender, age, economic status, race and etc. (ibid). The targeting can take place on search engines based on keywords, clicks, and IP address and it can also be in social media based on user profile information, interests, behavior and "likes". The thing about online advertising and targeting is the ability to narrowcast or microcast the audience which means that ads can be led to *individuals* rather than groups (Cohn, 2016, p. 681). And the valuable user data are traded by advertisers and come back to individuals as more personalized, automated and comprehensive ad recommendations (ibid, p. 677). In this way, advertisers have the ability to know their audience better and have power to decrease their *advertising waste* –which was the case in traditional advertising- thanks to information technology and society. Hence, targeting individuals becomes more efficient and cost saving[21].

In order to make targeting more accurate and efficient, platforms are collecting a huge amount of user data. For example, Google specifies which information they collect in their privacy policy. They describe two ways of collecting information: information users provide (such as personal information, name, e-mail address, telephone number or credit card number) and information they get when users use their services (*device information* such as hardware model, operating system, unique device identifiers, *log information* such as search queries, telephony log information like calling-party number, time and date of calls, duration of calls, IP, device event information like crashes, system activity, browser type, browser language, date and time of user requests and cookies identifying browser or Google Account, *location information* by using GPS, IP and other sensors (such as nearby devices, Wi-Fi access and cell towers), *unique application numbers* and *cookies and similar technologies* (Google, n.d.-a). Google says that they use information collected from cookies and other technologies "to improve user experience and the overall quality of their services" (ibid) which is just "a euphemism for saying that Google sells users data for advertising purposes" (Fuchs, 2011). Google says that their "automated systems analyze user content (including e-mails[22]) to provide personally relevant product features such as customized search results, tailored advertising, spam and malware detection" (Google, n.d.-a) which is just

[21] As Joseph Turow mentions in *The Daily You: how the new advertising industry is defining your identity and your worth* (2012) that "through data analytics processes, individuals are turned into individual evaluations" and also "calculations of each person's marketing value are produced based on behavioral and other forms of data tracking where each individual is categorized as target or waste" (Kennedy, 2016, p.47). As a result, not only advertising that are not targeted or micro-casted is considered as waste, but also people who do not comply with the expectations of the advertisers and their strategies.

[22] Google reads the content of the personal e-mails. For example, if a user has a flight, Google reminds it on the day of the flight by reading the e-mail of the purchase. It even warns about traffic jam, telling the exact time when user should leave home in order not to miss the flight. It also reads mails for targeted advertising (Hern, 2017). However, Diane Greene who is the CEO of Google Cloud states that "G Suite's Gmail is already not used as input for ads personalization, and Google has decided to follow suit later this year in our free consumer Gmail service. Consumer Gmail content will not be used or scanned for any ads personalization after this change" (Greene, 2017). However, it is important to notice that the act of reading the content of the e-mails continues.

another way of saying that they are “exploiting user data for economic purposes (Fuchs, 2011).

As ads are the backbone to make Google services “free of charge” and to make the company earn money, it is important to understand how they use cookies and how they work with their partners. As Google states “cookies help to make advertising more effective. Without cookies, it’s harder for an advertiser to reach its audience or to know how many ads were shown and how many clicks they received” (Google, n.d.-b). Websites, blogs or news sites partner with Google in order to show ads to visitors. And by working with partners, Google uses cookies for many reasons: to stop showing the same ads, to detect click frauds and to show ads that are more relevant (based on website visits) (ibid). Google serves these ads in their logs which are consisted of web request, browser type, IP address, browser language and cookies, and they reserve these data to *improve* their services (ibid).

“To help partners manage advertising and websites” (ibid), Google offers many products such as Google AdWords, AdSense, Google Analytics and DoubleClick which means that if a website shows ads by using these products, many cookies will be sent to user’s browser to track, to profile and to target (ibid) [23].

So, what does it really mean, how does it affect? It means that Google and its *partners* determine which ads user will confront. For example, based on a user’s location, a movie can be promoted on YouTube which will be soon on the theatre in user’s country. Or a search for ‘coffee’ can be turned into a suggestion of coffee houses nearby. It also depends on the context of the search. If a user is looking for health diet, s/he can see ads for health products. It is also possible that users’ activity on apps or Google services may lead to ads on the web. That is to say, if s/he uses any Google

[23] By using Google AdWords, clients and partners of Google can target ads based on search keywords, location, language, device, audience (such as gender and age) (Google, n.d.-c). When a person types a keyword and searches information, the message of advertisers which is relevant to the keyword typed by the user will be shown to users. If the user clicks on the relevant ads and visit the website of the advertiser, then the advertisers makes a payment to Google. The advertiser can also choose to whom to show the ads based on location, gender, age etc. They can microcast their audience to sell the product better. Another product is AdSense which allows publishers to place ads on their websites which are relevant to their content and audience (Google, n.d.-d). However, Pasquinelli criticizes that “Google’s AdSense provides a light infrastructure for advertising that infiltrates each interstice of the web as a subtle and mono-dimensional parasite, extracting profit without producing any content (Pasquinelli, 2009, p. 7). Google Analytics and Double Click will be covered later under the title “Behavior Market”.

service on phone, it can show her/him ads on the computer regarding the activity. Also, it is possible that an ad can be served by Google, but selected by another company. This means that if a person is registered with a blog, it can make decision about which ads to show and it can use Google's ad serving products to deliver them based on the information user provided while signing up to that blog. It is also possible to see ads on Google products/services (Search, Gmail, YouTube etc.) based on the information user provide to advertisers and which are then shared with Google (Google, n.d.-b). Therefore, advertising becomes a further mechanism which "advances the monopolization of business, manipulation of needs and the commercialization and commodification of culture and life" (Fuchs, 2011).

As a result, there are some important causes. The first concern is about users' privacy, because the data collected, traded and monetized can be personal, sensitive or even if it is non-personally identifiable information, it can *tell a story* about the lives of the users. People may think that it is not really important if platforms collect, track and monetize their search about random or mundane things. People might think their data are not important. However, this idea is so wrong. It is because mundane searches on their health, orientations or on any private issue will not be a secret but will be used to be sold to advertisers[24]. Second point is that people are exposed to "economic surveillance" where people are not empowered or do not have much to say regarding the use of their own data (Fuchs, 2011). That is the characteristic of many platforms. The third point is the asymmetry of power between platforms and users. Power relations between platforms and users are not symmetric and this causes several threats such as ideological, political and economic centralization threats and surveillance (ibid, 23). So, what should users do? Should users opt out of those platforms? Should they decide not to use? Should they delete their accounts? And also, is it possible to completely remove

[24] On selling the personal & sensitive data to advertisers, Google says that "when showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health" (Google, n.d.-a). However, later they continue explaining that "we may combine personal information from one service with information, including personal information, from other Google services… Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google" (ibid). Therefore, it is not clear what they do with personal or sensitive information. Also, it is too obscure and difficult to understand their terms considering that many people do not have that much time to clarify their practices on privacy. And even if users read one of the privacy agreements, it does not matter. Because it is nearly impossible to keep up with them, as they are changing all the time (Skeggs, 2017).

one's existence from these platforms? Or, should platforms need to take initiatives regarding user's decisions on privacy, commodification, monetization and exploitation?

User may use Adblock which is an extension to block ads for web browsers such as Google Chrome, Apple Safari, Firefox, Opera and Microsoft Edge. It allows users to block advertisements from being shown. According to 2017 Adblock Report, "%11 of the Internet population is blocking ads on the web (Cortland, 2017, p. 4). However, there are some polarized attitudes towards ad formats between users. That is to say, Adblock allows non-interruptive ad formats[25]. Also, a similar extension called Adblock Plus does not block third party tracking[26]. Moreover, there is a case which allows tracking even if the visitors use Adblock[27]. Apart from that, there are some options regarding the control on privacy and ads settings on Google. Users can use Ads Settings to control and manage Google ads that they see. However, this form of control is only adding up to Google's profit from ads, as it only helps to remove or add topics that users do not like to see and wants to see[28]. Also, they enable users to opt out from seeing ads personalization. However, just after giving this option, they state that "even if you opt out of Ads Personalization, you may still see ads based on factors such as your general location derive from IP address, browser type and search terms" (Google, n.d.-b). Therefore, the power asymmetry is still actively effective. Another important point is that if users block cookies on browser, including the services of Google, many of their services do not function. This means that their quality of service decreases (Google, n.d.-a). For example, if a user blocks location history or limits access to location, then Google Maps do not operate properly. It is also possible to manage users' own data by Google Activity which includes web & app activity, location history,

[25] According to the report, "77% of the Adblock users surveyed indicated that they found some ad formats to be permissible… Interruptive ad formats are the primary cause of user frustration, while non-interruptive formats, such as static banner ads or skippable video ads are broadly accepted" (Cortland, 2017, p.14).

[26] As stated in their website, Adblock Plus does not disable tracking automatically; that is to say, it is not figured to disallow tracking by default (Adblock Plus, n.d.).

[27] Even if the visitors use Adblock to disable Google Analytics tracking or even if they block JavaScript and Cookies in browser settings completely, tracking is still possible due to some PHP and some extra lines in JavaScript code (Matthees, 2017).

[28] From Google Ad Settings/Ads Personalization, users can see how ads are personalized for them and how they can control their personalization filters.

device information, voice & audio activity and YouTube search & watch history of the users[29].

As a result, there are some measures that users can take in order to protect their data from surveillance, trade, commodification and exploitation. However, as stated in the examples, these features do not give full authority and power to users to disallow tracking and commercialization completely. It stems from the fact that the business model of the Internet and platforms are based on advertising and commodification of data. However, another field that targeting and commercialization of user data happens is on the search engines and in their algorithms, which *rank* web sites and in return which results in search engine optimization technologies (SEO).

One of the major examples of algorithms that ranks websites and contributes to SEO technologies is the algorithm called PageRank developed by Google Search which ranks websites in search engine results[30]. It has been an important measurement defining the value of the websites. PageRank algorithm works "by counting the number and quality of links to a page to determine a rough estimate of how important the website is" (Web Archive, n.d.). Therefore, there is an "underlying assumption that more important websites are likely to receive more links from other websites" (ibid). As PageRank "describes webpages according to their popularity, [this situation turned search engine] into a hierarchy of results according to their rank" (Pasquinelli, 2009, p. 4). According to Matteo Pasquinelli, PageRank has a social component related to ranking of common intellect and it is based on the idea of attention economy. In attention economy, value is

---

[29] For example, regarding voice & audio activity, it is stated that "Google voice search records and keeps conversations people have around phones" which means that "the company is quietly recording many of the conversations that people have around its products" (Griffin, 2016). On this issue, Google states that it "records users' voice and other audio, plus a few second before, when they use audio activations like saying "OK Google" or tapping the microphone icon". It is also stated that "audio can be saved even when users' device is offline" and they further explain that by "using users' voice, they help to get better results by learning the sound of users' voice, learning how they say words and phrases, recognizing when they say "OK Google" and also by improving speech recognition across Google products that use users' voice" (Google, n.d.-e). Therefore, things that might have been said in private can be a part of Google's optimizing policy.

[30] Even though the last PageRank algorithm update was done on 5-6 December 2013 (Anderson, 2013), it does not mean that the algorithm is dead. It means they are not updating the Toolbar PageRank which was a tool to show the ranks externally and helped people to understand the rank / value of their domain. Therefore, it is not public anymore, but it is still working internally (Yodania Group, 2016). And, it can be assumed that Google is still using it to determine the value of a web page or site on the Internet.

given to products which get more attention. Thus, results at the top of PageRank get more attention than the other pages. This means that pages with a higher PageRank will be more visible to human consciousness and curiosity. He describes that PageRank is a "mechanism… for setting *rank value* for each node of the web" and "*rank value* set by Google is… recognized as the currency of global attention economy and crucially influences online visibility of individuals… companies and… their prestige and business" (ibid, p. 7). As a result, it is important to realize that Google is not only exploiting human knowledge by ranking what is important but it also extracts value from human life and transforms it into network value (ibid, p. 3-4). According to Christian Fuchs, the ranking algorithm is a way of surveillance which is searching, evaluating and indexing www[31] (Fuchs, 2011). He points that Google is benefiting from the expansion of the web as people create content on the web, even though it does not pay for using web content as a resource (ibid). The idea is that the more content and web sites are on the www, the more Google has to index in search results. And in return, the better search results people get, the more likely that people come across with matching ads that they may click (ibid). In other words, Google's ranking algorithm is benefiting from the user-generated content and the expansion of the web by indexing them in the search results to provide more relevant ads which people might be interested. Also, it is not only deciding which information to be delivered and to be presented to human consciousness, but it is also deciding the *visibility* of the web pages and web sites by ranking which web site to be at the top of search results. And in order to gain this visibility, web sites are employing SEO marketing strategies.

Search engine optimization is a strategy of internet marketing and it happens by optimizing a website which can be editing the content of it, practicing HTML or coding to increase relevance of the website for keywords and etc. The thing about SEO is to understand how people search and to understand what kind of result the search engine wants to show to users (Anderson, 2018). Frank Pasquale discusses that it is odd to compete search results, as they are thought as the web's neutral map. Are they really?

[31] He explains that the details of the algorithm are not transparent to users. However, it works in this way: Small automated programs which are called web spiders search www, algorithm examines all the pages that are found, it counts how many links the page gets, it further identifies keywords for each page and eventually ranks its importance (Fuchs, 2011).

Because the industry based on search engine optimization reveals the pressure individuals and corporations suffer “as they struggle for salience in results associated with certain queries” (Pasquale, 2011, p. 245).

Therefore, it is important to realize that optimizing technologies have decision-making features which are not only resulting in information diet (how information is presented to human knowledge by ranking systems, how algorithm decides which information has more importance than the other), but it also results in some other important consequences. The first one is *prioritization.* Nicholas Diakopoulos states that prioritization “serves to emphasize or bring attention to certain things at the expense of others, such as when a search engine prioritizes and ranks the most relevant search results” (Diakopoulos, 2015, p. 400). And the criterion in algorithms to prioritize involves choices and value-propositions which can be political, biased and ideological determining what gets to the top (ibid, p. 401). And when these criteria are not public (which is the case most of the time), then it becomes nearly impossible for users to understand what contributes how. The second consequence is the *visibility* of the search results which affects corporations economically. Hannak et al. points “ranking certain results higher or lower can dramatically affect business outcomes” (Hannak et al, 2013, p. 527). In order to be visible in the ranking, corporations are employing SEO strategies “to be found, indexed, and displayed more easily” in the search results (Mager, 2012, p. 776). Also, being visible to the right audience is as important as being visible in the search result rankings (ibid). Otherwise, marketing a product would have no meaning, if it were made *visible* to the wrong audience. The third result is considered as *consumerism*. It is believed that search engines and optimizing technologies are corresponding to dominant culture of consumerism (ibid, p.778). It can be called consumerism, because there is a shift in the society from being producers to consumers and search engines are corresponding well to this shift as their business model is based on advertising (ibid). It is because “new needs need new commodities; new commodities need new needs and desires” (Bauman, 2007, p. 31 as cited in Mager, 2012, p. 778). Therefore, it can be concluded that “capitalist spirit is embedded in search algorithm by ways of social practices” and it should be concluded that both online service providers and user are in this together which means that they are "stabilizing the technology with their marketing, search and consumer practices" – consciously or unconsciously- (ibid, p. 779).

1.3.3. Behavior Market

Behavior market, as defined by this thesis, is a market based on behavioral targeting on the web. Behavioral targeting is defined as making use of the "user's browsing habits to influence ads selection" (Guha, Cheng & Francis, 2010, p. 84). It can be conducted on search, website or online social networks. And what is meant here as *behavior* is user's "browsing behavior, recent searches and recent clicks on products" (ibid, p. 85). And considering the profiles on the social networks, there are two factors that affects the behavioral advertising; user's gender and age (ibid). Therefore, behavioral advertising can be described as "a broad set of activities companies engage in to collect information" about user's online activities to show ads / content that are relevant to that particular user (TrustArc, n.d.). In order to achieve this, companies also use cookies to collect data about user's browsing activities and these cookies are stored on the user's computer when they visit web sites (ibid). Behavioral targeting enables advertisers to map user's interests based on web sites / page they visit, the content they read / click and many other actions they perform online (ibid). So, one person may ask: What do they really know about people? Or, how much information & what kind of information do they use? It is emphasized that the data collected for behavioral advertising are not connected to users' personal information (ibid)[32]. This means companies collecting user data do not tie it to their personal information such as name, surname, address, e-mail address, but they try to identify a person by ID number and try to define interests or

[32] Personal Information is defined by European Union Data Protection Directive 95/ 46 /EC as: "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (European Parliament & Council of EU, 1995). As it is seen, the definition of personal information of EU is a very broad one. Name, surname, e-mail address, telephone number, address etc. are directly identifiable information, but the situation of the information such as IP address remains obscure, as it is not clear in the definition if it is personal or not, or if it can be personally identifiable. Also, different countries have different opinions on what should be considered as personal information. For example, IP address may be treated as personal information in Canada (Himo & Carron, 2016), whereas USA has more of a sectoral approach to privacy of data (Lambert, 2016). Therefore, it is believed that the issue whether IP address is personal information creates more concern if it is used for behavioral targeting and advertisement.

characteristics of a person based on his/her online activities and the data that are tied may consist of age, gender and purchase interests (ibid).

However, behavioral advertising may have benefits for some users such as "the free online content that advertising generally supports and personalization that many consumers appear to value" (Federal Trade Commission, 2009). But privacy concerns come along with the 'potential benefits' of behavioral targeting, as it is a form of tracking. The first concern is the fact that data collection is invisible to users (ibid). Users are not aware that their data or how much of their data are collected for what reasons[33]. Therefore, it can be deducted that the ignorance is achieved by the users, too. The second concern is that the collected information (which can also be personal or sensitive concerning health, sexual orientation, finance etc.) may fall in the wrong hands or can be used for other purposes than it was anticipated (ibid). The third concern is that the tracking of the user data for behavioral advertising can result in exploitation, commodification and monetization of social relations, intimacy and habits. As a result, it can be deducted that behavioral targeting has a nature consisting of both monetization and surveillance; tracking and advertising go hand in hand / accompany each other from a sectoral perspective.

Therefore, one question that needs to be asked is: what happens when intimacy, relationships and habits are monetized? (Skeggs, 2017, p. 5). What happens when social interactions are monetized? How frequently do your data monetized? If you are reading this thesis with anything open on computer, it is very likely that you are being evaluated, traded and tracked: Per second, 100.000 requests are made from advertisers to access to your data, and 50 billion times a day, bids are made to access your data by the advertisers (ibid, p. 3). In 2014, Facebook placed 52.000 unique data signals to one profile, and as if this is not enough, it buys other data to enhance that profile (ibid). Also, if you are a high networked / high net worth person with influential (a great

[33] Even though it is suggested that personal / sensitive data are not subject to behavioral advertising most of the time, users can never be sure if that is the case. It is because the business model of the Internet and many platforms are designed to make use of users' personal data. For example, considering the business of these platforms, one can easily find out that they are actually not producing a great amount of stuff. So, what do they do? They rent users the space –renting profiles to users- on their platforms and this rent is paid for not by the user, but by their right to users' personal data. And this happens, when users sign the "I agree to use this" privacy policies (Skeggs, 2017, p. 18).

number of) friends, then it is more likely for you to be tracked faster and valued more (ibid, p. 4). Facebook and many other platforms are using machine learning algorithms to try your data to match with relevant advertisers; you provide signals each time when you become online and use Internet such as e-mails, videos watched, messaging, browsing, device used, webpages / websites, speed of connection, location, history data, networks (ibid)… So, what are you going to do? You can turn off your social networks, you can opt out from platforms or you may have never used Facebook, but still you are being evaluated, traded and tracked! Therefore, turning off or opting out are not solutions[34]. So, one question should be asked is that: "Is there anything beyond capital" (ibid, p. 5)? Is there really anything left that is not monetized, traded, exploited, commodified or surveilled for the capital? Therefore, it is important to realize that new forms of capitalism are not only working on us, but also *through* us" (ibid, p. 37).

Why behavioral advertising is important? Because it is based on habits, and this is why the new forms of capitalism are not just working on us, but through us. Commodification of human habits though analytics / prediction[35] enable companies to have new canals –meaning new commodification opportunities- where they can act on.

[34] Even if a person has never signed up to Facebook, s/he can still be tracked by Facebook, if s/he is visiting a website / page that has Facebook symbol. It is because of the fact that "when a user visits a third-party site that carriers one of Facebook's social plug-ins, it detects and sends the tracking cookies back to Facebook" (Skeggs, 2017, p. 16). In June 2015, Belgian government tried to block non-user tracking of Facebook. Even though Facebook denies it at first, they reveal later that they are actually doing it. It is also found that Facebook's opt-out option enables tracking. However, Belgian government lost the case against Facebook, because Facebook is registered in Ireland which means that Belgian court do not have international jurisdiction over Facebook based on Ireland (ibid). Therefore, Facebook still continues to track and trade non-users.

[35] One of the remarkable analytics tools is DoubleClick which is an advertising server of Google collecting and networking data from websites on usage behavior and it sells this data to provide targeted advertising. In order to network the data, it also holds the data related to the user's browsing/usage behavior from other web platforms, too (Fuchs, 2011). As a result, "connecting with right people, in the right moments" (DoubleClick, n.d.-a) and serving ads and "managing it all seamlessly from a single platform" (DoubleClick, n.d.-b) mean that Google is using the server of DoubleClick to collect user behavior data from the www and use it for targeted advertising (Fuchs, 2011). Therefore, it can be concluded that the economic surveillance and exploitation of the user data is a networked one which spreads all over the www (ibid). Another analytics tool that is highly used for behavior targeting is Google Analytics. It is a tool that is all about gaining new insights about the data. As they suggest "big data can come with big challenges" (Google, n.d.-f), they aim to make companies to know their audience, find the best matching content and optimize their ad inventory (ibid). It also works with AdWords, AdSense, DoubleClick and other Google products to make companies understand how their *customers* behave on sites / apps. It helps companies to get access to "Google's proprietary audience data" spanning through the Google networks which allows creating audiences that are based on demographics / interests (ibid). That is an open way of saying that they are exploiting and commodifying user data. And later, audiences of these data will be used for campaigns.

Analytics is important for behavior advertising, because it helps to make sense of dozens of raw data and helps to understand one person's behaviors which are engrained in her/his habits. Habits are important part of behavior market, because daily habits influence people's decisions. And, with predictive analysis methods, companies can target their audience's habits at the right moments so that they can develop their business with these strategies[36].

As a result, online behavioral advertising is about the ability of the companies to think like how their customers think and look at where they are looking at. It is about the ability of single data point to mean something at societal level, when collected and analyzed[37]. It is about the ability of the algorithms to revolutionize what companies

---

[36] One example of this is from the supermarket called *Target*, because analytics of user data is not only limited OSPs, but also to offline world markets. Target is a supermarket which is aware of the fact that when people's habits change, their habits of shopping change, too. Therefore, they looked for times when people might have major changes in their lives that can affect their shopping habits. In other words, they looked at times when people are "vulnerable to intervention by marketers" (Duhigg, 2012). One of those times is during pregnancy and birth of a child. By crawling the user data, they found a "pregnancy prediction" score which help them to estimate due date of the baby and stages of the pregnancy. For example, they found that pregnant women buy unscented lotion at the beginning of their second trimester and in the first 20 weeks they take supplements like calcium, magnesium and zinc (ibid). A year later of pregnancy prediction model, a father of a high school girl walks into Target and demands to see the manager for the coupons that were sent to his daughter. He was angry at the company for sending his daughter coupons for baby clothes and products, accusing the company for trying to encourage her to get pregnant. When the company checked the mailer, it was sure that his daughter was on the list for maternity clothing, nursery furniture etc. The manager apologizes and calls later to apologize once again. However, this time, the father owes an apology for the manager, as he was unaware of the activities in his house –after a talk with his daughter, it turns out that his daughter is actually pregnant-. Therefore, the data are powerful. When analyzed and made sense of, they can tell stories about people –which can be even sensitive, intimate, private or personal-. And companies are looking ways of accessing these personal narratives to leak into people's decisions. When asked, target declines to describe what demographic information they collect or purchase, but they claim that they comply with all privacy laws (ibid). However, they are very well aware of the fact that if they send a pregnant woman mails or catalogs about baby stuff who did not register herself as pregnant, she may feel herself *spied on.* Therefore, they are mixing the personalized ads with random stuff so that advertised products would look like they are chosen by chance (ibid).

[37] A data point which is considered as *unimportant* by the user actually has an economic value and becomes a part of the economy. Some people say that 'how my data can have a value', 'how my online meal order can affect my shopping behaviors' or 'why data of an *ordinary* person like me should matter". As a result, they can consider their data 'not very important'. But it is very important to realize that regardless of the importance attributed to data by the user herself/himself, the data have an economic value itself. For example, Yemek Sepeti which is an online meal ordering service shows how *every* user data are powerful, resourceful and efficient source of value. They state that by evaluating the results of the football matches or by following TV series' broadcasting times, they can comment on the differences and changes in their users' meal order actions. They compare the differences between Google search data and their own order data, and in this way, they foresee the trends in the eating habits of people (Marketing Türkiye, 2016). Also, they mention that Yemek Sepeti can analyze how sales change in a profitable day with evaluation of meteorology data. In this way, they can even prevent the customer dissatisfaction by automatically narrowing some areas of service during heavy snow (ibid). Therefore, a single data point or

know about people and how precisely they can sell, as a result of the conscious or unconscious patterns that people render into data sets (Duhigg, 2012).

There are some consequences of online behavior targeting which raise ethical concerns. Standardizing user's online behaviors, suggesting purchase, remarketing a product[38] includes "unseen, categorical, computational judgements about which searches, articles or purchases should *probably* come next" (Ananny, 2016, p. 103). So, the users are not only subjected to commodification of their data, but also they are subjected to limited options that are offered to them. That is to say, there is a "categorical resemblances among objects" that are purchased or searched (ibid). The second concern is the uncomfortable feeling of being spied on. However, people seem they feel uncomfortable if the companies seem like they know a lot about their past behavior, but it becomes acceptable again, if the advertising or economic tracking perfectly aligns with people's interests[39] (Wohn & Sarkar, 2014, p. 577). The third concern is that ideas,

---

a single meal order maybe cannot tell much of the story. However, when many data points are collected and analyzed, they can tell a story. Similarly, if a great amount of data of a user analyzed together, it can tell about a person's likes, tastes, tendencies and preferences. And in turn, these can be used to advertise and market further. Another example can be Twitter. The tweets that lead to trending topics on Twitter are evidence that small data points have a great impact at societal level when aggregated and analyzed. Because a single data point may not have effect, but when they are accumulated under the same hashtag, they become powerful enough to create a trend and to communicate an idea. Trends have societal effect in terms of economy, too. It is because trending topics can be read as "index of what is said and an advertisement to read further" (Gillespie, 2012). Measuring the phenomena (trends) can be considered both as a feedback and also as a feedback loop, because it is possible to make use of and discuss further something that trends (ibid). That is to say, advertisers can develop strategies for their business by following and analyzing the trends on Twitter.

[38] Remarketing is a strategy which *helps* websites to *reconnect* and to reach users who interacted with their business so that websites can advertise their product when users search, visit other pages and use other apps (Google, n.d.-g). In this way, websites can show relevant ads to users if they leave the website or mobile app without buying anything and it also works when user adds a product on the shopping cart but not complete the transaction (ibid). It also enables websites to reach users on their remarketing lists as they browse more than 2 million websites or mobile apps (ibid). For example, if you look for a shirt on online shopping website, but decide not to buy it, this is the reason why you see that shirt hunting you through the web, in other websites and wherever you go.

[39] It seems that people are likely to feel disturbed when companies know about their sensitive data and use them. However, it also seems that people do not mind the fact that their personal information/data are known and used, if it benefits them such as sociality, finding their path on the web easily, getting similar recommendations on a subject which can enrich them and etc. In return of using the services, paying with their own personal data do not irritate people, if they make use of the services and if the economic surveillance is not too much. That means if they are made to feel safe and protected enough by the companies; it seems to them 'okay'. However, the mentality of "what you do not know, will not hurt you" is a wrong one, as companies are finding ways to make users feel like "not spied on", but actually know everything about their consuming habits and practices. And, consuming habits and practices is not only

experiences and feelings of people are transformed into a quantifiable value for the market (Hearn, 2010, p. 433). As a result, the intimacy, affiliation, affection, social life and relations are commodified by transforming them into databases. The forth concern is the "database of intentions" (Battelle, 2005, p. 1). Behavioral data are used by marketers to interact with the users through *database of intentions* where user information is used to understand intentions such as purchase intentions and also general social needs/desires. The last concern is "marketing discrimination" which happens when "marketers increasingly use computer technologies to generate ever-more-carefully defined customer categories –or niches- that tags customers as desirable or undesirable for their business" (Turow, 2006, p. 1 as cited in Beer, 2009, p. 990). This means that establishment of these niches about consumers can lead businesses to treat different customers according to different niches in order to profit, increase efficiency or for anything (ibid).

1.4. SURVEILLANCE

Imagine a world in which employers have the data to predict candidates' health condition and their future well-being based on data points which are extracted from their social networks (Acquisti, 2014, p.76)[40]. The power of data can enable employers to make decisions without the awareness of the candidate based on these predictions which may end up not hiring someone whose life expectancy is considered as low (ibid).

Imagine a world where users' online behavior exposes their preferences/habits and companies can estimate precisely what they need and offer their products to users in the right time. Based on the analytics of data, companies are able to tell differences in the shopping habits of newborn baby's mum versus six-month-old baby's mum and one-year-old's mum (Garett, 2015) and they are able to make mums gain new habits by targeting and selling them products which they are not even aware they need.

used in the meaning of shopping, but it also includes a wide range of consuming activities performed online such as reading, listening to music, learning how to cook and many other mundane activities.

[40] This narrative story is inspired by the article of Alessandro Acquisti (2014) called The Economics and Behavioral Economics of Privacy.

Imagine a world in which public officials has the access to citizens' personal and private data such as Internet data, phone records, bank and credit cards records from third parties such as Internet providers, telephone companies, credit card companies and banks (Clarke, Morell, Stone, Sunstein, & Swire, 2013). And based on these data, it becomes possible for governments to monitor neighborhoods to predict where and when a *potential* crime may happen.

Imagine a world in which every part of daily life is turned into databases to profile users so that they can recommend things, estimate habits, sell products and affect decision-making processes better. Based on these social data, people's activities can be used for companies' strategy of identity formation and reading consumers further. Mundane activities like watching TV series can be used to identify consumers as gay or not (Cohn, 2016, p. 675) and daily activities on users' social networks can be part of an experiment to read their emotions (Goel, 2014).

While people continue to carry out activities through the day, they leave so many digital bread crumbs behind them, because the ubiquitous digital world of data is available in so many aspects of life (Greenwood, Stopczynski, Sweatt, Hardjono & Pentland, 2014 p. 193). Analyzing and making sense of the patterns through these digital bread crumbs is called "reality mining" (ibid; Eagle & Pentland, 2006). By analyzing the data obtained from many people about a single subject[41], it becomes possible to explain things that are unpredictable such as social movements or revolutions (ibid). Also, it becomes possible to understand who is likely to get certain illness, who is likely to pay debts or who is likely to commit a crime. As a result, these digital bread crumbs that people leave behind are keys to who they are, what they do and what they want (ibid). And this situation makes personal data so valuable which *contributes* to different components of the system; personal data provides economic value and it also provides

---

[41] Greenwood and friends make a difference between the data of actual activities such as records of call data, transactions data of credit cards, GPS locations etc. and the data gathered on social networks as these data on social networks are edited by people. That is to say, posts, shares or likes on social media are what people prefer to tell. They are kind of filtered to match the persona people want to create on social networks. Therefore, social networks can tell and provide insights about human nature, but their value is limited for more operational things like optimizing. On the other hand, the *actual data* which are not edited can directly tell what the person is engaged with, what the person looks for or interested in (Greenwood et al., 2014, p.193)

transparency[42] to monitoring organizations. In the previous chapter, it is explained how economic tracking creates value. And in this chapter, it will be discussed how tracking and monitoring for surveillance creates value. This phenomenon will be supported with the theory of *Panopticon* which is considered as fundamental in surveillance studies. However, it will be explained with a twist and a reversal which is brought by the means of the information society such as social networks, Internet and computation.

1.4.1. Reversing the Panopticon

What does the idea of Panopticon –which is a big part of surveillance studies- mean in the digital data culture? Can it still be related and applied to datafied society? What will be the implications?

It would be better to start explaining the legacy of the Panopticon. It is first developed by the social theorist Jeremy Bentham. The design of the panopticon expresses the system of control of an institutional structure. The design of panopticon allows inmates to be observed by a watchman who is situated in a place where all inmates can be observed, but they cannot tell whether they are being watched or not. As inmates do not know if they are watched continuously, they behave as if they are under watch all the time. And, this results in controlling the behavior of the inmates constantly.

Michel Foucault used panopticon as a metaphor which operates as a power mechanism in disciplinary society. Panopticon refers to the tendency to observe. It addresses how observing normalizes for the people. According to Foucault, effect of the Panopticon is "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault, 1975, p. 201). This means that the effect of the surveillance remains permanent, even when the action does not continue (ibid). It is described as a discipline machine to dissociate the see and being seen: while the one in the periphery is seen without ever seeing, the one in the center sees everyone and everything without ever being seen (ibid, p. 201-202). That is to say, the prisoner (metaphorically) is seen, but he does not see; while he is an object of information, he

[42] Transparency is used here in the meaning of "being explicit". It means personal data to be read by monitoring organizations easily; it addresses the ability of the monitoring organs to analyze, create patterns and surveil the data which reveals details of interaction and life.

never becomes a subject in communication (ibid, p. 200). And in information society, surveillance finds its logical reasons that people can normalize and embrace the monitoring and tracking of their actions: People can be surveilled, because “morals are reformed, health is preserved, industry is invigorated, economy seated and etc.” (ibid, p. 207).

On the Internet, “visibility is a trap” (ibid, p. 200). Just like in the panopticon metaphor of Foucault, subjects can be monitored, surveilled and tracked on the Internet. The surveillance (of the state or private companies) can be totally invisible to individuals, and in this sense, the issue of visibility is similar to Foucault’s idea of visibility (McMullan, 2015). Also, there is not a watch tower on the Internet, but there will be *sensors* which will communicate with each other even in individual’s intimate objects (ibid). In this sense, the communicating sensors in the devices can be considered as the watch towers of today.

However, it is believed that the metaphor of panopticon is reversed. One thing that is reversed is the view on the exposure of bodies to surveillance. While browsing on the Internet, individuals do not feel themselves exposed as it happens in the panopticon. It is because people do not have so much attachment for their data, as they do for their physical bodies (ibid). The second thing is that people who are surveilled are there voluntarily. That is to say, people put themselves on the Internet or on the social networks willingly to be visible, while being visible by the system in the metaphor of panopticon is not something demanded, but forced. The third thing is that while the metaphor of panopticon aims to control and surveil the behavior of those surveilled, the reversed panopticon demands people not to be similar but to perform their characteristics and behaviors. It is because reverse panopticon creates *opportunities* for the advertisers and private companies on the Internet to catch people who fits their market best.

Moreover, considering the social networks, there are more issues that can be reversed. First of all, on the social networks, the system does not act upon the users from above. This means that the system which is based on the algorithms of the social networks are not acting upon the users above, but it also enables interaction from the below, and more importantly the power also rises from the interrelations between the users which is not the case in the metaphor of panopticon (Bucher, 2012, p. 1172). The second point is that there is no single permanent gaze on social networks (be it newsfeeds, home pages or channels) that monitors people under the same gaze (ibid, p. 1171). Instead, there are many different gazes which monitor each other. The third point is that the possibility of being observed all the time is not a problem on social networks, while it is the main problem in the metaphor of panopticon. However, on social networks, the problem is the possibility of being disappeared from the flow (ibid). The fourth point is that while the metaphor of panopticon equally subjects everyone to permanent visibility, social networks do not subject everyone equal visibility, it prioritizes some people's visibility above others as a result of ranking algorithms. As a result, visibility is not permanent and ubiquitous as in the metaphor of panopticon, but rather it is temporary and scarce (ibid, p. 1172). Therefore, visibility does not function as a punishment as in the notion of Foucault, but rather it functions as a reward (ibid, p. 1174). As a result, the idea of reserved Panopticon is a voluntary, desired, scarce and demanded phenomenon on social networks and on the Internet. After establishing the theory of Panopticon, the concept of *dataveillance* which best explains the changing surveillance practices on the platforms will be discussed with examples.

1.4.2. Dataveillance

Surveillance is itself a very broad term. There are many different types of surveillance such as physical surveillance, electronic surveillance, behavioral surveillance, bodily surveillance, personal surveillance, mass surveillance and many more. And, there can be many different reasons for surveillance such as economy, security, identification, health, crime prevention and etc. However, this thesis particularly looks into surveillance which is performed on personal data and which intrudes informational privacy leading to loss of control over personal information.

In relation to this, the study has a scheme to examine areas where surveillance over personal data happens. The scheme includes: Surveillance over *private life* which means surveillance over health, welfare, confidential information (credit card, phone number, ID etc.); surveillance over *economy* (commodification of data & habits of shopping, behavior market etc.); surveillance over *security* (predictive policing, crime prevention etc.); surveillance over *social life* (social networks & online platforms). The scheme that is drawn here is based on the activities of individuals performed on OSPs. This means that surveillance over private life, economy, security and social life will be examined only when they are performed on the platforms provided by OSPs. Otherwise, it will exceed the boundaries of the study. And, the best matching term that conceptualizes the purpose of this chapter is believed to be *dataveillance.*

Dataveillance is first described by Roger Clarke as “the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons” (Clarke, 1988, p. 499). Clarke coined the term in the mid-1980s in order to draw attention to a shift that “occurred from (expensive) physical and economic surveillance of individuals to (cheap) surveillance of people’s behavior through the increasingly intensive data trails that their behavior was generating” (Clarke, 2018). And what makes dataveillance ‘cheap’ is the *automation* of the surveillance of data.

Since then, the theory of dataveillance developed in many ways. One concept that has been developed is “digital persona” which means that it is a “model of an individual’s public personality based on data and maintained by transactions, and intended for use a proxy for the individual” (Clarke & Greenleaf, 2018). Those who developed the theory make a difference between physical surveillance and the persona of the dataveillance. While physical surveillance is about individual’s body and behavior, dataveillance “watches the shadow that the person casts as they conduct transactions, variously of an economic, social or political nature”[43] (ibid). The other argument is about giving control to the individual of the digital persona who represents it (ibid). Another development in theory was realized by taking into consideration of some specific techniques such as profiling, data matching, monitoring of search terms, articulated models of interaction, location & tracking data, analysis of dataveillance’s support for authoritarianism, political freedom and effect of the big data movement have shaped the integration of dataveillance into a broader set of concepts (ibid).

[43] “The shadow that the person casts” can be thought here as data doubles which is described by David Lyon as the software identity, digital identity or as the data subject. It is considered as an important representation and a component of the actual identity that is gathered by the data trails of the person. This addresses the electronic profile of the persona that is created on the databases –which is the shadow of the actual person that fulfills the agency of doing (Lyon, 2007; Binark & Altıntaş, 2016, p.317).

There are two kinds of dataveillance described: personal and mass. While *personal dataveillance* is described as *"*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of an identified person", *massive dataveillance* is described not for identified person, but for "groups of people" (Clarke, 2016). It is mainly conducted to identify individuals who share or belong to particular interests.

Dataveillance can comprise of some techniques such as *front-end verification, computer matching and profiling.* Front-end verification means "the cross-checking of data in an application form, against data from other personal data systems, in order to facilitate the processing of a transaction"; computer matching means "the expropriation of data maintained by two or more personal data systems, in order to merge previously separate data about large numbers of individuals"; profiling is described as "the technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics" (ibid). The techniques are not limited to that, but they can be considered as the basis of the technologies applied today.

And in this part of the study, the concept of dataveillance will be discussed with examples to show how it is performed in people's lives through private life, economy, security and social life. Monitoring private life over personal data can happen in any part of the private life. However, it has enormous impact when the data that is surveilled is about health. In his article "Personal Health Data in the Reality of HIV", Nejat Ünlü from Positive Living Support Center in Turkey shares important results of stigmatization and discrimination that come along with the datafication of health records of HIV[44]. He states that people with HIV are even afraid to go to test centers, as

---

[44] However, it is important to discuss –as argued in the article - that datafication of health records of HIV is not the thing that causes stigma and discrimination. It is the system that keeps records of personal and sensitive information of the individuals in a vulnerable and open way to third parties (health workers, Ministry of Health workers, pharmacists, insurance companies etc.). And actually, datafication or keeping records of the HIV illness is regarded as something positive, because only in this way the illness can be controlled and people can get the help they need. However, in order to achieve this, people first need to feel themselves comfortable to share their sensitive information, and this requires the government and health workers to create a system where sensitive and personal data of the patients are not shared, sold and used.

they are recording name, surname, ID number; they are afraid of this information to be known. And even some doctors request prophylaxis medicines from Positive Living Support Center, as they do not want this to be seen in register of the patient with HIV (Ünlü, 2016, p. 142). Also, the system called 'Medula'[45] is a system that causes anyone to find out personal information about a patient, because it is enough to know the ID number of a person to access all the list of medicines that a patient has received (ibid, p. 143). And because of this, people are getting their prescriptions from other places than they live in order not to be recognized as HIV by their neighborhood (ibid, p. 143-144). Moreover, the system called e-nabız[46] is another software that does not care enough about informational privacy of the patients. In the default settings of the application, the personal information is open to anyone to be read easily, while it needs to be other way around (ibid, p. 144). Also, when a person is diagnosed with HIV in Turkey, a form with a code is prepared for this person. With this code, the patient can be tracked by Ministry of Health, but it is not possible to understand whose code is that. However, they demand to remove the code and prepare the form in a way which can directly depict the name and surname & ID number (ibid). And also, Ünlü tells that some patients (not HIV patients, but other patients in Turkey) get messages (kind of ads) right after the treatment and prescription about the medicine they will use. He states that it is not clear how they get the number. The situation is scary, because Positive Living Support Center is providing the data they have when needed, and they are afraid of these data to be sold (ibid, p. 145). Privacy of these data is very important, because this is vital for those people to continue their lives. Therefore, privacy of personal data is a very crucial step that needs to be taken care of, because these people face marginalization and maltreatment, they are refused from treatment, they lose their jobs and they are forced to lose their status in life (ibid, p.143).

As surveillance over economy has been discussed earlier under title "targeted advertising and behavior marker" quite intensely, rather than exemplifying it once again, it would be better to discuss it together with surveillance over social life, as they

---

[45] It is a system that is designed for pharmacists to enter prescriptions.

[46] It can be translated as "e-pulse" and it is a system where patients, doctors and Ministry of Health workers can access the data about the person's illnesses, prescriptions, tests and other health records.

are well integrated into each other. Mundane activities that people carry out in their lives such as using social networks to communicate ideas or watching TV series on the Internet by using streaming media such as Netflix can be a part of the economic tracking and monitoring of social life. Considering the Netflix, it is argued that removing information that can identify individuals is not enough to make them anonymous (Narayanan & Shmatikov, 2006-2008:11 as cited in Hallinan & Striphas, 2016, p. 125). It is further discussed that more intimate and private aspects of an individual's identity can be inferred such as political & sexual orientations, religious leanings and even body type (Narayanan & Shmatikov, 2006-2008:16 as cited in Hallinan & Striphas, 2016, p. 125), and this is supported by Jane Doe v. Netflix lawsuit which took place after the Netflix Prize contest[47]. Jane Doe, a lesbian mother, "feared to be outed as a result of having rated numerous gay and lesbian-themed titles through Netflix (Hallinan & Striphas, 2016, p. 125). Basically, the mother was disturbed by "her movie selection and rating transactions to be included in any public disclosure of data" (Jane Doe v Netflix, 2009, p. 21). As discussed, "were her sexual orientation public knowledge", it is thought that "it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's ability to live peaceful lives within [the] community" (ibid). Monitoring of social life and economy is integrated here, because the better the algorithm recommend, the more users will continue to watch movies and use Netflix. And this will contribute to the profit of the company. Disclosure of user data for a competition can reveal individual's preferences of their private life which results in monitoring some aspects of their social lives.

Another example where surveillance was performed over social life is from social networks. In January 2012, Facebook reported that they changed the number of positive & negative posts in the news feeds of 689.003 users which are selected randomly in order to see what kind of effect the changes will have on the posts that were shared later by the recipients (Goel, 2014). The result of the study was that the people who saw positive posts tended to write or share more positive posts, and similarly those who saw

---

[47] The Netflix Prize was a competition which "sought to substantially improve the accuracy of predictions about how much someone is going to enjoy a movie based on their movie preferences" (Netflix, 2018). In order to achieve this, contestants were expected to develop an algorithm that can recommend movies better.

negative posts tended to be more negative in the posts they share (ibid). The company not only manipulates people's news feed, but it also exploits people by giving the users more of what they prefer to see so that users will spend more time on their services and will see more ads –which constitutes most of the revenue of the company (ibid). This is a good example where surveillance over economy and surveillance over social life integrates.

One of the notable examples of where dataveillance is performed over security is predictive policing for crime prevention. Police department of New York uses 'predictive policing'[48] algorithms in order to "combine historical crime data with real-time data, geo-located tweets, deploying officers" in order to find out "where and when crime is most likely to occur" (Morrison, 2014 as cited in Ananny, 2016, p.106). The system is like a crime forecasting which tries to guess where the crime is most likely to happen. The system aims to prevent the crime before it happens, and this sometimes leads to situations where there is no crime, but the algorithm thinks a crime *might* happen and targets individuals in a biased way. For example, prediction software analyzes the criminal risk scores which give people scores from one to ten to understand whether they are likely to commit a crime in the future or not and it depicts that it was biased towards giving high scores unjustifiably to black defendants (Eubanks, Angwin & Nelson, 2018). As a result, one person can ask if algorithms or human judgement are worse when it comes to discrimination and bias, because there are counter ideas that algorithmic predictive policing can be a solution for discrimination as they are considered as 'neutral' and 'transparent'. However, it is believed that algorithmic predictive scores cannot be regarded either as transparent or anti-discriminative. It stems from the fact that algorithmic predictive scores are running the data which are provided to them -which already have human bias in it. That is to say, if you give the software the data that are biased, the outcomes of the algorithms will be -unsurprisingly- biased, too. And in this case, it is believed algorithms may be worse than human judgement and decision-making, because they concretely systemize the bias and also, they hide the bias which results in automated inequalities (ibid).

---

[48] Predictive policing is "the application of analytical techniques- particularly quantitative techniques- to identify likely targets for police intervention and prevention crime or solve past crimes by making statistical predictions" (Perry, McInnis, Price, Smith & Hollywood, 2013, p. xiii).

It is believed that there are some ethically problematic consequences of dataveillance and surveillance of personal information in general. The first is one *disempowerment.* In a system where every aspect of individuals' lives is increasingly monitored, people feel themselves disempowered to express ideas, to communicate with each other and to take control of their own data. It is not only about losing privacy, but it is about losing self-determination and power (ibid). The second one is *discrimination.* In a system where algorithmic decision-making operates on the biased data, it is no surprise that algorithms make decisions which are based on already existing biases & prejudices in the society such as ethnicities, colors of people and economical status. Therefore, it is believed that machine learning algorithms are further contributing to discrimination. And in return, this is leading to automated algorithmic inequalities. The third one is *invasion of privacy*. Monitoring, exploiting and monetizing personal data or sensitive data are believed to be causing invasion of privacy in many aspects. The information people want to keep private or data that they think companies or services are protecting are actually sold, used and monitored like a commodity. The forth one is *power asymmetry.* Individuals' control over data is so little when compared to how much control companies or governments have, and it is believed that this is creating power asymmetry. People expect governments to protect their data in the cyber space and audit private companies to be sure if there is no violation. However, it is also no solution, because governments are also buying and selling data of the citizens. And people again feel themselves powerless, when the government is in their data too much. Then, who is going to protect them from the government? Therefore, instead of looking for some institutions to take care of personal data of the individuals, it is believed that people need to have control and power over their own data in the first place in order to prevent power asymmetry. As a result, it is believed that this brings out the questions of one person's right to privacy, control and access regarding the ownership of her/his own data.

1.4.3. Privacy, Control and Access

Privacy, control, access and power are all about user data. In information societies of today, data are important, valuable and resourceful asset that can not only shape, affect and drive economy, scientific research, business, welfare, but also influence issues such as governance, security or surveillance (Taddeo & Floridi, 2016, p. 1594). Therefore, regulating who access data when is an important issue, because it is about finding a balance between interests of the society and progress of the individual rights (ibid). And in this regard, privacy plays an important role, because data trails –little digital bread crumbs- of users reveal a lot about their preferences, health, economy and social life. And online service providers (OSPs) which often obtain and have access to personal data of the user stand between the data and the powerful agents intending to have access to such kind of data such as governments, companies or even OSPs themselves, because they are also interested in user data –be it personal or not- (ibid, p. 1595). As a result, there are some questions emerging; who should access personal data and information of the users? What should be the balance between privacy, control and access? What do privacy, control and access mean for users and powerful agents? What should OSPs do in order to act responsible for "accessing, controlling and managing users' data" (ibid)?

Thinking privacy with some other concepts such as power, control, access and autonomy helps to develop different perspectives while characterizing the privacy. It is important to understand how *access* and *control* are related to the concept of privacy. It is defined as a form of control and also it is described in terms of access (Nissenbaum, 2009, p. 70). In this sense, "privacy is a condition that is measured in terms of the degree of access others have to you through information, attention, and proximity" (Gavison, 1980 as cited in Nissenbaum, 2009, p. 70); or it can be defined as "the condition under which other people are deprived of access to either some information about you or some experience of you (Reiman, 1976, p. 30 as cited in Nissenbaum, 2009, p. 70). In this condition, privacy is described in terms of access; it is measured by how much access others have about you or how much information they are deprived of. On the other hand, privacy as a form of control is described as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7 as cited in Nissenbaum, 2009, p. 71); and it is also described that "privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves" (Fried, 1968, p. 482 as cited in Nissenbaum, 2009, p. 71); or it is "the ability to control the acquisition or release of information about oneself" (Froomkin, 2000, p. 1464 as cited in Nissenbaum, 2009, p. 71); or it is "an individual's control over the processing –i.e., the acquisition, disclosure, and use-of personal information" (Kang, 1998, p. 1203 as cited in Nissenbaum, 2009, p. 71). This thesis adopts the definition of Charles Fried which means that privacy is not only the absence of information about us in other people's mind, but privacy means to have control over what information other people have about ourselves. It is because information is power. And claiming the *right* to have control over which information to be given to others also means having *right* to privacy and control of the *power* and this empowers individuals in the system full of power asymmetry.

However, there are also studies which hybridize the issue of control and access. Anita Allen defines three dimensions of privacy: physical privacy, informational privacy and proprietary privacy (Allen-Castellitto, 1999, p. 723 as cited in Nissenbaum, 2009, p.71). This thesis study is particularly interested in *informational privacy* which is characterized by "confidentiality, secrecy, data protection and control over personal information" (ibid). Even though, this study adopts "privacy as a form of control" model, it is important to realize that degree of the access to information is also very crucial regardless of who is in charge of control. Both approaches have important aspects of the privacy, but it is thought that the control model fits the purpose of the thesis better in terms of *agency* and *empowerment* of the individual.

Considering the agency of the individuals -which means control over their personal information or data-, it is thought that "people have [the] right to control information about themselves" or to limit access to information about themselves (Nissenbaum, 2009, p. 72), as this serves individuals interests better than having a sectoral approach to ownership and control of data / information. Privacy – control relation also brings into mind the relationship between privacy and autonomy. It will not be wrong to tell there is a connection between privacy and autonomy; there are two reasons for this. The first reason is that "if privacy is understood as the claim or right to control or determine access to information about oneself, then autonomy can be "understood as self-determination", meaning that actions of the individual are governed by the person with her/his principles (ibid, p. 81). That is to say, it is about the ability to perform self-determination regarding one's own information (ibid). The second reason is that control over information/data about oneself (like controlling which information to be used, having a voice about the ownership of data, deciding to be or not to be monetized, commodified or tracked) leaves a room for freedom of speech (because individuals feel free to express themselves without hesitation only when they are in charge of their own data and when they are not exposed to commodification and surveillance). As a result, it can be deducted that freedom of speech comes along with self-determination and it empowers individuals to be autonomous of their action.

1.5. CONCLUSION OF THE FIRST CHAPTER

As a result of the first chapter, it is concluded that algorithms are not only technological, but also cultural and societal constraints. They are affecting how culture and cultural practices are experienced and how daily life is regulated. It is argued that sophisticated features of algorithms creating complex and subjective results. It is discussed that how algorithms and their features are used by companies and governments for which reasons are creating social and cultural problems.

One consequence is about consumption of information. It is discussed that algorithms have become effective in selection and delivery of information on services provided by OSPs. Algorithms are acting like gate keepers by editing which information to be on top, omitting posts of friends whose content is not found relevant and deciding what to show first on newsfeed. It is concluded that this situation is narrowing the world view of people, enabling them to see things that are similar to their world view and content. As a result, this situation leads to a culture which continues to conform itself, but not confronts with different ideas (Hallinan & Striphas, 2016). This is important, because it is argued that this can possibly decrease the ability of criticism in the society.

This also effects the reality construction. Users seeing posts of their friends who share the same world view or users who come across with news that are similar to their point of views will be entrapped in different realities. This means that people will start living in different bubbles, and they will not be able to see other people’s ideas and other contents. And, this will result in the fall of public sphere, because there will not be shared experiences left. When there are no shared realities, then the society starts to be separated and to be divided inside.

Removing human choice and automating the editing of the algorithms are believed to be causing homophily on social networks. In real life, people tend to meet, associate or bond with people that have similar characteristics and personalities, too. However, people have the chance to come across with people holding different ideas and experiences. Due to ranking and personalization algorithms, people are deprived of the choice to select what to see and what not to see. Therefore, it is creating a loop where people surrounded with similarities and it is believed that this is increasing the homophily on the social networks.

Regarding the economy politics of algorithms, it is concluded that free service policies of platforms are creating an illusion. While people get entertained, read news, connect, share, like, communicate or get information, they are paying with their data in return of ‘free’ usage of the services of OSPs. It is argued that data has become an economic input of the modern information societies. Therefore, when people create content on the Internet, it becomes free prosumer commodity which is an opportunity for platforms to index more.

It is discussed that OSPs have created monopolies on the Internet with their multitude of services and with their services spreading on the web. That is to say, these service providers expand their business by creating multiple types of applications ranging from education, entertainment to information (such as maps, social networks, mail etc.), and they also made it possible to sign up different web sites with their accounts. As argued, this situation is leading to platformization and dominance of OSPs on the web. It is also revealed that big service providers’ purchase of small applications and start-up services contributes to dominance of OSPs.

Data which are discussed as the new oil, new currency and air of the information societies are considered as a powerful and a resourceful property which has the ability to tell about insights of person’s preferences, tastes, habits, tendencies, fears, life styles and etc. It is argued that companies and third parties are looking for and developing ways to capture this data to sell their products better by targeting advertisements on the Internet and social networks. As a result, ownership of data is at stake, because data are shared, abused, exploited and sold like a commodity. Also, it is revealed that micro-targeting the audience, communicating ads not for groups, but for individuals leads to consumerism. By predicting behavior, companies become capable of manipulation. It leads to consumerism, because knowing exactly what target audience demands, needs and prefers will create new needs and habits for people.

Regarding the surveillance, it is concluded that digital trails people leave behind contribute to tracking of personal data which is valuable not only for the companies, but also for the governments. In the name of security and optimizing services, governments and companies are collecting too much data about their citizens and users. It is argued that there is an asymmetry between people and data holders in terms of power. Mining, analyzing and collecting user data are believed to be causing loss of control and power. One example of this is seen when people sign privacy agreements of the service providers. By accepting the terms and conditions, people give their consent to commodification and exploitation of their data, and this consent paves the way for power asymmetry. It is also noticed that default settings of the platforms and their services are not protecting the users. Even the systems that hold personal and sensitive data such as healthcare demand too much data of the users and they sell or share these data with third parties such as advertisers, insurance companies and workers. This is leading to violation of sensitive and personal data. As a result, default settings of the OSPs are found abusive, while it needs to be other way around and protect people's privacy and provide their right to confidentiality.

It is found out that invasion of privacy also means loss of freedom of speech. People can express ideas, only when they feel themselves safe to communicate, and it is only possible by providing people's right to privacy. If there is no privacy, then people prefer invisibility of their ideas, practices and problems. For a better society where people communicate counter-views, issues and questions freely and openly and for a healthier communication, it is argued that it is necessary to provide people confidentiality.

However, the concern and reaction of people towards tracking and surveillance practices by companies and governments shows variety in an interesting way. People seem to be concerned, when governments or companies know a lot about themselves and manipulate them with targeted news and ads. However, people seem to be less concerned or even not care at all, if the companies serve towards their benefits. That is to say, if economic tracking and usage of data bring benefit for them, then it is considered as okay. However, if companies target them with their secrets, then people are scared of the amount of the information companies or governments hold about them. Thus, it is revealed that people start questioning the ownership of their data, their right to access and control of the data mostly in extreme conditions.

The last conclusion remark is that people may lose human autonomy in decision-making processes, as they are handed to algorithms. And algorithms which are working on data may create biased results. It is because data that are given to algorithms have human touch which means that they are already biased. As a result, the output the algorithm produce is a biased one, too. However, there is one thing at risk. When algorithms are making decisions, they are automating them. This means that algorithms continue automating biased results which leads to discrimination and separation in the society. As a result, it is thought that automation of algorithms creates an algorithmic system which furthers the prejudices in the society.

1.6. EVALUATION

This part aims to make a general assessment of the chapter, emphasizing approach of the study for discussions and providing points to connect it with the following chapter.

The chapter derived from the question ‘how features of data-driven algorithms and related practices affect culture and society’. This study approach algorithms as not only technological, but also social and cultural constraints which are answering more complex and subjective questions for us. It is determined that there are three main fields where impacts of algorithms can be observed. These were conceptualized as: information diet, economy politics of algorithms and surveillance.

With regard to information diet, it is understood that algorithms are creating a taste for users in relation to information consumption and they are acting as gate-keepers which edit, omit and select which information to be delivered with their decision-making features. Also, it is discussed that personalization algorithms are creating filter bubbles which leads to narrowing of world views and people are entrapped in eco chambers where automation of algorithms stabilizes homophily on social networks, leading users to be deprived of choices. In return, it is argued that this decreases shared reality and experiences of the public.

With regard to economy politics of algorithms, it is discussed free service policies are merely illusions where people pay actually with their data. Data as the main economic input of information societies are highly desired by the companies. It is argued that online companies are leading to dominance and platformization with their business structure. It is argued that data is considered as a powerful tool by companies, as it is indicative of human conduct and it is a great story teller. It is considered that targeting and micro-targeting activities of companies are leading to consumerism and resulting in economic surveillance of users. Predictive analytics on behavior is believed to be leading manipulation.

With regard to surveillance, it is discussed that digital trails people leave behind are key to who they are. Data collected in the name of security is believed to be leading to loss of control and power. Lack of access to personal data may cause data asymmetries. It is also discussed that default settings of the companies are abusive, as they are arranged to gain maximum profit from the users. Moreover, there is a correlation between freedom of speech and privacy. It is discovered that people can express themselves only when their privacy is ensured. Apart from that, it is discussed that automated algorithms are stabilizing and hiding bias in the systems which may affect the outcomes of predictions which are made for the sake of security and policing.

Thus, this study asks what users, citizens and individuals should do in the face of emerging problems that are discussed here. This study is of the opinion that technology will continue to develop in a very fast paced way. Companies, governments or any other data rich entities that hold power will look for the ways of increasing their profit and consolidating their strength. Therefore, this study asks, what would be the action of users, citizens and individuals for these challenges? The study suggests data ethics as a response, aiming to start an ethics discussion before the ‘unethical’ is stabilized.

CHAPTER 2

DATA ETHICS

Data are great. Data science can benefit the society with its promising potential and capacity, provide more efficiency or opportunities and contribute to the solutions of the emerging problems which are experienced in information societies. However, it can also cause harm.

As users, we would like to be connected with friends and families. We would like to communicate our stories, share our moments of life and be creative with the content we publish. We would like to perform our art in the mediums that are given to us in the digital world of today. However, as users, we also wish our contents to be visible to people who are different than us, with whom we are not likely to encounter in real life, if it was not for the social networks[49].

As consumers, we would like companies that we interact, make purchases from and use their products to have insights about us. We would like to be important and valuable. We would like to receive relevant discounts or suggestions about the services we are interested in. We would be glad if we get a discount from an airline company for the route that we commute most or for an item that we need most. However, as consumers, we also wish to be informed about the use of our data and to have a clear understanding of how they are monetized and commodified, and the consequences of targeting individuals based on their own preferences, habits and interests.

As customers, we would like to find similar contents on the topic that we search, read, learn and entertain. We would like to expand and deepen our knowledge with recommendations that are similar to our mindset. We are happy to get more articles about our research topic and this will eventually save time on literature review. We enjoy getting recommendations for similar movies of our taste. However, as customers, we also wish not to be trapped into a commercial loop which aims to increase

[49] This narrative story in the beginning of this chapter is inspired by the "Data Science Ethics" course given by H.V. Jagadish.

companies' profit by giving customers similar content so that people will spend more time on their services and eventually provide them with more customer data.

As patients, we would like medical treatments to advance by making use of data patients provide. We would want scientists to find a better treatment or a cure for a particular disease. We would be glad if value and meaning are extracted from our health data for better scientific results of a disease. However, as patients, we also wish patients' right to privacy to be ensured and taken care of. We would not want our sensitive health records to be abused and exploited. We would be scared that our health data may fall into wrong hands or that it would be public without consent and anonymization.

As citizens, we would like any crime to be prevented without causing any harm or resulting in casualties. We want our neighborhoods and parks to be safe and legal; we would like to feel free to be mobile in cities. We would be glad if police departments develop an algorithm or software to detect terrorist acts before they happen. We would embrace a technology which can protect woman or young girls from assaults. However, as citizens, we also wish these technologies to be fair. We want our probabilistic and predictive systems to make fair decisions and we would like fair treatment before being punished with a particular crime.

As decision-makers, we would like to get advices from data-driven algorithms. We would like to have the value they create out of huge amount of raw data. We would want algorithms to help us in decision-making processes such as hiring and employing people, as we tend to believe that they are more *neutral* than human judgement. However, as decision-makers, we also want to prevent "unintended bias" (Jagadish, 2016). When trying to be neutral, we do not want to experience bias which occurs as a result of human touch in algorithmic designs and data-sets.

And, as people, we would like to play with technologies and express our art by trying new possibilities. We want to dare to create new systems for our society which we believe to be beneficial and harmless. We would like to make use of all the possibilities that information society provide us and we want to innovate. However, as people, we wish not to be discriminated by data-driven algorithms based on color, origin, gender, age and economic and geographic status. We want our data models to be diverse and inclusive so that algorithms can come with more resourceful outcomes.

Therefore, it important to realize that there are possible unintended and undesired outcomes of data-driven algorithms such as invasion of privacy, discrimination, bias, ossification, commercialization and many others. So, as users, consumers, customers, patients, citizens, decision-makers and people, what will be our action? Should we opt out from these platforms and services for the fear of losing our human values? Should we be scared to use new technologies? It is believed that answer is no. There will always be new problems emerging from the possibilities of the new technologies when we try to make use of their capacities. There will always be pitfalls along the way. However, it is believed that there is something else we can do. We should not necessarily avoid these technologies, but we should rather start discussing ethics of data science in order to gain control and agency in our lives. Therefore, it is believed that it is important to ask below mentioned questions to understand the scope of data science ethics and to improve accountability and responsibility of OSPs, by beginning an ethical discussion about the impacts of the technologies they create.

2.1. UNDERSTANDING DATA ETHICS

In this section of the thesis study, an ethics discussion is started in order to define the concerns surrounding data-driven algorithms and to analyze their impact on society, culture and everyday life. It is hoped that this discussion will eventually contribute to and build on existing discussions on the field and offer insights for the issues. This part aims to answer these questions; what is ethics, what is data ethics, what does ethical algorithm mean, what is the ethical approach of this study and why is it important to study data ethics now?

2.1.1. What is ethics?

Before getting into discussing data ethics or ethical algorithms, it is better to start with ethics itself theoretically. The question of what ethics is has a history of 2.400 years old literature and it is not an easy one to answer. Therefore, it is important to know where to begin and how to handle this broad topic. The discussion will first start with the definition of ethics, and then three ethical theories which are considered as *workable* for the thesis and the questions they address will be explained theoretically in the *traditional* sense. Afterwards, these traditional perspectives and the questions posed by these theories will be applied to technological field to find out what they will mean and if they will be relevant.

Each community or society has some set of rules about what members of that community should do or not do in different situations they experience in life and this is called *morality* (Quinn, 2014, p. 51). And, this is the reason why people who live in different societies have different morals for situations and ideas. For example, this can explain why there are different approaches and applications around the world regarding the GDPR. While data protection or regulation may have utmost importance for one society and for its members, it can be secondary for another. This is because what people value differs from one society to another. According to John Dewey, moral theory is "the analytic perception of the conditions and relations in hand in a given act, -it is the action *in idea*. It is the construction of the act in thought against its outward construction. *It's, therefore, the doing, -the act itself, in its emerging"* (1891, p. 188). And ethics is defined as "the philosophical study of morality, a rational examination into people's moral beliefs and behavior" (Quinn, 2014, p. 51). It is essential to emphasize that it is based on reasoning, so people need to explain, compare and discuss why they hold their ideas or conduct dear. Similarly, John C. Merrill describes ethics as "the study of what we ought to do" (2011, p. 3). According to H.V. Jagadish, ethics is about shared values of a society/community (2016). Therefore, the idea of "what we ought to do" is not related to whatever a person thinks as ethical –in other words, it does not stem from a person's arbitrary, random, subjective will (Uzun, 2011, p. 327)-, but it is based on shared values of the society. And it is important to notice that ethics focuses on people's voluntary and moral choices (Quinn, 2014, p. 55). That is to say, ethics forms the base of the rules people follow voluntarily (Jagadish, 2016). Anything that is involuntary does not concern ethics. Therefore, ethics is not law, because law and morals are not the same. However, laws follow ethics and laws enforce ethical behavior (ibid). This means that if someone does not behave in an ethical way, this does not mean that s/he breaks the law. However, laws look up to shared values, concerns of the society and demands of the society members and make law from the morals. As a result, ethics makes the basis for laws.

Having defined the ethics, it is time to discuss the three models that are considered as workable for this study: they are deontological, teleological and the virtue model belonging to normative ethics methods. Normative ethics is concerned “with criteria of what is morally right or wrong” (Normative ethics, n.d.). That is to say, it tries to develop the criteria which enable to evaluate the actions within the framework of morals before identifying them (Uzun, 2011, p. 23). Therefore, normative ethics is about examining the questions which occur while thinking about what and how should a person ‘ought to act’, or basically how actions or life should be.

Deontological model is about basing ethical thought or actions on principles and maxims which are considered as *guides* for those actions (Merrill, 2011, p. 11). It is about following rules, duties, maxims or principles (ibid). It is believed that following these rules is the key for behaving ethically, if you break them, then a person is unethical. For example, citing and giving reference to an author in our original work is a code which is expected to be followed in academia. If s/he does not, then it means s/he is unethical. It is because deontology is regarded as the knowledge of moral values or rules that needs to be followed while performing a profession (Uzun, 2011, p. 21). And, deontological approach is mainly associated with German philosopher Immanuel Kant. According to Kant, actions and behaviors of people should be guided by moral laws which are universal and based on reasoning (Quinn, 2014, p. 67). The morality criteria for an action cannot only be the consequences, but it is based on other principles such as decisions, honesty, justice and respect for people and property (Uzun, 2011, p. 24). However, how do we know if something is good and what is good? It is because qualifications which are considered as good can also be used in a way that can harm others. And for this dilemma, Kant asks “what is always good without qualification?” and he answers that “the only thing in the world that can be called good without qualification is a good will” (Quinn, 2014, p. 68). So, what he says is that something that results in good or produces value is not what makes something good. What makes something good is the “good in and of itself” (ibid). That is to say, good will is good on its own. Furthermore, Kant describes that following what we ought to do, instead of what we want to do is *dutifulness* (Beck, 1997 as cited in Quinn, 2014, p. 68). In an action performed out of respect for the duty, the moral value is not found in the goal which will be achieved with it, but in the maxim which decides to do it (Uzun, 2011, p. 24). Therefore, a dutiful person behaves in accordance with moral rules. But he also formulated categories to guide the duty and action which is called *categorical imperative*. This would describe if moral rule is suitable to follow. The first one is "act only from moral rules that you can at the same time will to be universal moral laws" and the second is "act so that you always treat both yourself and other people as ends in themselves, and never only as a means to an end" (Quinn, 2014, p. 68-69). The first one is about asking if a person would like her/his moral rules to be universal. That is to say, is it okay, if everybody acts in the same way? If a person universalizes her/his action and moral thought, and if it is not in a logical contradiction, then it can be assumed that it is an appropriate moral rule or duty to follow. The second one implies that using someone or using oneself to reach a goal does not comply with the categorical imperative. It draws attention to the point that everyone is a rational being and should be treated as ends in themselves, but not as a means for an outcome. As a result, deontological model is good to object instrumentalization of people, to have a more humanistic approach and to test agreeableness of moral rules, but it can also cause harm if the duty-to-principles are followed without reasoning.

Teleological model is about focusing on the consequences in contrast to deontology. Teleology is a result-oriented approach that describes the actions on the basis of their good or bad consequences (Uzun, 2011, p. 23). And, this model is generally associated with the English philosophers Jeremy Bentham and John Stuart Mill who think that "an action is good if its benefits exceed its harms, and an action is bad if its harms exceed its benefits" (Quinn, 2014, p. 73). Their theory is called utilitarianism which is based on the principle of utility and which is also called as the Greatest Happiness Principle (ibid). So, according to utilitarianism, the criterion that defines the good and the bad is not the goals, but the consequences. In other words, in utilitarian ethics, the aim is to choose "the action that will bring the most good to the party the actor deems most important" (Merrill, 2011, p. 11). And the actor that is defined here can be herself/himself, or as in the case of Mill and Bentham, it can also refer to society. That is to say, utility is "the tendency of an object to produce happiness or prevent unhappiness for an individual or community" (Quinn, 2014, p. 73). As a result, an action is considered as right/wrong, as much as it increases or decreases the parties' total happiness, and the moral action is then defined as the one which generates utmost happiness (ibid). To sum up, morality is not related to the aim behind the action, because morality can only be measured in its effects. Consequently, it is a workable approach, because it focuses on happiness, it is practical and comprehensive (ibid, p. 75-76) and it requires reviewing all possibilities before taking action and thinking about the consequences of an action (Uzun, 2011, p. 25). However, it is also important to note that "not all benefits have equal weight" (Quinn, 2014, p. 75), and it may also become reductive when qualities such as goodness and happiness are reduced to mathematical quantities (Uzun, 2011, p. 25). Therefore, it can be hard to calculate the happiness and to find out the best, but it provides a comprehensive understanding of the situations.

Finally, virtue model is neither about duties or principles to follow or consequences of an action, but it is about "reaching one [person's] highest potential" (Quinn, 214, p. 89). While the other two models emerge from the Enlightenment, this one dates back to ancient Greece and works of Aristotle which is called *Nicomachean Ethics,* and according to him, "the path to true happiness and genuine flourishing as a human being lies in living a life of virtue" (Aristotle, 1998 as cited in Quinn, 2014, p. 89). That is to say, virtue ethics is based on the idea of virtue and habitual practice of virtuous behaviors (Merrill, 2011, p. 14). According to Aristotle, there are two types of virtues and these are intellectual and moral virtues (Quinn, 2014, p 89). While the former is related to reasoning or truth, the latter is about virtues of character, habits or dispositions which are gained by repeating the virtuous acts (ibid). Therefore, the moral virtue is described as a "deep-seated character trait" which needs not only acting in a certain way, but also needs a disposition to *feel* in a certain way (ibid). In other words, people are not born with moral virtues, but they come into exist in people as they practice the virtuous acts and turns them into intellectual virtuous habits (Merrill, 2011, p.14). Furthermore, according to Hursthouse who is considered as neo-Aristotelian, the key to be virtuous is to have a virtuous character which means forming dispositions needed to perform virtuous actions and they are considered as an indication of good inner states of a character (Hursthouse, 1999 as cited in Tonkens, 2012, p. 141). Similarly, Hursthouse considers virtues as character traits that support flourishing and flourishing is a needed achievement to live a good life (ibid). Therefore, humans need to act in accordance with virtues and avoid acting viciously (ibid). Acting viciously or a vice is described as “a character trait that prevents human being from flourishing or being truly happy. Vices, then, are the opposite of virtue” (Quinn, 2014, p. 91). According to Aristotle, the vices can be excessive or defective; it is about avoiding the extremes and looking a rational and a moderate stand point for ethical thinking and decision-making (Merrill, 2011, p. 15). To sum up, virtue ethics is about asking what kind of person we should be, instead of thinking what we ought to do in ethical problems (Anderson & Anderson, 2007, p. 19). Instead of focusing on duty or consequences of actions, virtue ethics is about the moral character of the agent, and it can be deduced that character of the agent is the base of the moral understanding (Tonkens, 2012, p. 141). So, a right action is the one that is conducted by the virtuous person and a virtuous person is the one that has and lives with the virtues and the virtues are the character traits that humans need to flourish and to be happy (Quinn, 2014, p. 90). Virtue model is a workable theory because it reduces the dilemmas concerning consequences or the duties to follow, it includes emotions and it helps to improve moral judgement of the individuals. However, there are also no guides to follow unlike deontology. Also, happiness or flourishing can mean different virtues to different people. Thus, it is hard to make a policy from the virtue ethics as it focuses on the individual. And, the character traits and the actions become secondary.

Having discussed the three ethical models for this study, it is essential to ask what these ethical approaches will mean when they are applied to technology. Will they be relevant? And, which questions will they pose? So, is it possible to implement the theories of ethics in an algorithm or in a computer system? (Allen, Wallach & Smit, 2006, p. 14). In other words, can moral theories lead algorithms/computer systems to be ethical, guide design of these assemblages, or promote ethical competence (ibid)?

Considering the deontological approach, it means technology to follow some set of ethical principles. It is possible to see the contribution of the deontological model to technological realm in codes of conduct, regulations, policies and standards which define the principles of developing technology ethically, showing engineering students morals of their professions, “teaching best practices, and preventing future failures”

(Ananny, 2016, p. 95). For example, there is *Ten Commandment of Computer Ethics* (Computer Ethics Institute, 2011) which provides engineers with duties and principles to develop technology ethically: there are human rights frameworks such as *Universal Declaration of Human Rights* and there is European Data Protection Directive and now GDPR, containing the privacy principle on implementing data regulation (SIIA, 2017, p. 4). And, of course, there are many similar examples.

Considering the teleological approach, it “tries to anticipate ethical concerns raised by technological innovation” (Ananny, 2016, p. 95). It is mainly because today technology is ever-growing in a very competitive and fast-paced environment that when companies/researchers push the limits or boundaries of technology, it is possible that there can be harm caused to users unconsciously. Therefore, there are institutions or organization preparing documents to make engineers think about the possible negative and harmful outcomes of their work and also to make them question the way they innovate. For example, AOIR provides researchers with charts on frequently asked questions about ethical practice (AOIR, 2017) or SIIA poses questions about data governance. And, it is worth to mention that these documents which draw attention to consequences of technological conduct are always subject to change. Therefore, this requires the awareness that we cannot apply existing ethical frameworks to reconfigure new relationships between the actors (Ananny, 2016, p. 95).

Considering the virtue approach, technology follows the values, virtues and beliefs of the people who develop the technology rather than codes of conduct, principles, duties or considerations on the consequences of a technology. It is possible to see contributions of virtue approach in technologists’ thinking of the technology itself: including “their own ethical standards” (Fridman, Kahn & Borning, 2006 as cited in Ananny, 2016, p. 95-96) in their designs and creations, deciding which values to integrate with the criteria of excellence and flourishing. These values, decisions or standards are not found in the codes, but in their own individual practices which means taking designer or technologist’s context as a primary unit of analysis (Ananny, 2016, p. 96). In other words, according to virtue ethics, ethics emerge from individual choices, understandings, preferences and point of views, not from the codes of conducts or institutional approaches (ibid). For example, this is reflected in Helen Nissenbaum's ideas of seeing privacy as a contextual integrity (SIIA, 2017, p. 4).

Consequently, it is important to understand that algorithmic systems are "moving targets" (Ananny, 2016, p. 108), and they are technological and social assemblages which means that as much as designers shape technology, technology shapes culture and human relations as well. They are not stable in their design, interactions and interpretations. Therefore, it is not possible to think about ethical dynamics of these assemblages with stable ethical standards. It is believed that this requires new dynamic perspectives that can develop from these ethical models. However, it is hard to imagine computing sense of social life, responsibility, duty, principle and reasoning into technological systems (Pariser, 2011b). These ethical models are helpful to question the ways to embody ethical discussions into technologies. Deontological approach can be useful to determine rules and codes to follow when applied to algorithmic systems, but it would be also hard to follow whether all parts of the system follow the duties and principles or not. Teleological approach can be helpful to focus on the consequences of these systems, but it is also important to think about accountability, opacity and transparency in a time where systems have learning capacities. It is also hard to focus on the consequences, when the systems are built together with the contributions of the users. It opens up new ethical questions on responsibility and accountability. Virtue approach is good to see each part of the assemblages "as a particular ethical arrangement", but it is also hard to understand and measure them "in the context of fast-moving, algorithmic assemblages with myriad, unseen code, actors and norm" (Ananny, 2016, p. 109).

As a result, it is important to ask what is needed. It is needed not to follow a single approach, but a mixture of all three approaches. It is needed to understand that any ethical consideration on technology should combine codes of conduct, comprehensive understanding and reasoning on the consequences of innovations and individual insights about design and value of the technologies. It is needed to realize that application of these ethical models to algorithmic systems is not comprehensive enough, when they are ever-growing, developing and having new capacities such as learning, deciding, prioritizing, recommending and regulating. Therefore, a perspective which can represent the new concerns that come along with algorithms is highly needed and it is believed that this can be found in *data ethics.*

2.1.2. What is data ethics?

The discussion will first start with the definition of data ethics explaining its traits, background and then it will focus on what it covers and how data ethics is relevant to today's information societies which are mainly governed by algorithm and data.

According to Floridi and Taddeo, data ethics is considered as a branch of ethics examining moral problems relevant to data (which includes generation, use, recording, processing…), algorithms (which include artificial intelligence and agents, robots and machine learning) and practices (which include responsible innovation, professional codes, programming…) to form morally good outputs (2016, p. 3). As a result of this definition, they formulate and conceptualize three axes for ethical dilemmas that emerge from data science, and these are "the ethics of data, the ethics of algorithms and the ethics of practices" (ibid). That is to say, they are providing us with the conceptual framework to study data ethics.

One question that needs to be asked is why data ethics? It is because there are computer ethics, information ethics, machine ethics, network ethics… Data ethics actually builds on the foundations of computer and information ethics which have focused on the challenges of digital technologies for the last 30 years (Bynum, 2015; Miller & Taddeo, 2017; ibid, p. 2). Studying technological ethical dilemmas posed by computers and information systems with data ethics is actually related to a shift which tells about the ethos of today's modern information societies. The shift is about "changing level of abstractions of ethical enquiries from information-centric to data-centric one" (ibid, p. 2). It focuses on various moral aspects of data: it puts an emphasis on the fact that ethical problems like "privacy, anonymity, transparency, trust and responsibility concern data collection, curation, analysis and use" before they concern information (ibid, p. 3). This shift also brings focus on all types of data, not just the data which equals directly to information, but also data which can be used to produce behavior or make sense of the actions (ibid, p.1). For example, a person's Facebook likes may not translate into information directly, but it can tell about her/his actions, make sense of the behavior and even produce behavior. The shift can also be explained with its focus on the *interaction* between software, hardware and the data, instead of the digital technologies that enable interaction (ibid).

So, what are the ethical problems posed by data science? What is covered? In other words, what is discussed as an ethical problem in data ethics? Floridi and Taddeo conceptualize these problems around the aforementioned three: the ethics of data focuses on collection & analyses of datasets, profiling, advertising, open data, re-identification of people via data-mining, trust and transparency: the ethics of algorithms focuses on complexity and autonomy of algorithms, moral responsibility, accountability of designers and data scientists, ethical design and auditing: the ethics of practices focuses consent, secondary use, user privacy, responsibilities of people & organizations who account for data process, policies and strategies and frameworks defining for professional codes (ibid, p. 3). Furthermore, in relation to ethical problems posed by data science and big data, Andrej Zwitter focuses on power, agency, control over data, free will and individuality (2014, p. 3-5). And these problems are observed in various activities and areas in social life: from search engines to social media platforms, online news, education, markets, political campaigns, urban planning, welfare, public safety, movie ratings, music recommendations, medical diagnosis, hiring and etc.

For the ethical problems of today emerging from algorithms and related practices, data ethics approach is thought to be relevant because of six reasons which can answer the needs and potential problems of algorithmic culture. Data ethics takes ethical problems more comprehensively and it is more inclusive. The first reason is that power relations are hyper connected and networked in socio-technological assemblages. Power is not distributed from one place and it is not linear. Also, "epistemic relations are power relations" which means that different agents (non-humans, humans) have different levels of power (Simon, 2013, p. 15). The second reason is that the concept of agency which is "knowledge and ability to act" and "capability [for a] morally relevant action" becomes "dependent on other actors" in a networked and interactive structure (Zwitter, 2014, p. 3). Also, it may result in losing agency to *act* compared to agents that have more amounts of power in the assemblage. The third reason is that knock-on effects[50]

[50] A secondary or an indirect effect.

play a major role in hyper-networked ethics which means that actions in a hyper-networked or connected structure increases the potential of collateral damage (ibid), because power can come from any direction and with different levels of agency and free will. The forth one is a result of the third and it is knowable outcomes. In a hyper-networked or connected structure, knowable outcomes reduce and unintended consequences increase, because the definition power changes (ibid). Also, prior to testing of an algorithm, judging or deciding to what extent the algorithm matches the predefined ethical rules or principles means attributing some *fixed* features and path to development of the algorithm (Neyland, 2016, p. 54). However, in a networked, ever-changing structure where the result of a design is unsure, it is not possible to have knowable outcomes. The fifth reason is the unstable nature of the algorithms. They are considered as “unstable objects of study” (Ananny, 2016, p. 109) which is mainly because of the fact that they are learning, changing and developing agents. The sixth reason is the ‘many hands’ problem (Zwitter, 2014, p. 2). It means “interactions among multiagent systems [that comprise] several agents [and which are] not all necessarily [always] human” (Floridi, 2013, p. 728). As there are many human or non-human agents contributing to a system/work, there is a distributed morality conducted by ‘many hands’. It is believed that all these above-mentioned reasons make studying the ethics of data and algorithms different, compelling and complex.

It is believed that there is a natural flow and transition from discussing data ethics to understanding the idea of ethical algorithms, because ethical practice of data affects ethical working of algorithms. And, an algorithm producing ethical outcomes is also bound to data it works on. Therefore, they are structures that are considered as interdependent to each other in producing ethical results. Also, as drawn in Floridi and Taddeo’s data ethics scheme (2016, p. 3), discussing ethical algorithms is a part of studying data ethics. Moreover, questioning the meaning of an ethical algorithm leads to a new set of issues such as free will, intentionality and responsibility of machines and artificial agents. Therefore, it is believed that it is necessary to uncover the meaning of ethical algorithms.

2.1.3. What does ethical algorithm mean?

Having discussed data ethics, it is time to focus on the procedure which works on the data, and it is algorithm. While studying and thinking about the research subject, explaining data ethics first seemed to be comprehensive enough to cover the meaning of ethical algorithm. However, after reviewing the literature, it seemed necessary to cover what ethical algorithm is and what we should understand from that under a title of its own. In order to understand the ethics of algorithms, this study looked at engineering ethics, machine ethics and computers ethics. The questions to be asked in this discussion are: is it possible to study ethics of algorithms; why do we discuss ethics of algorithms (what are the unethical practices / problems); what does it mean for an algorithm to be ethical, or what should we understand from ethical algorithms; how can an algorithm be ethical, or can it be? If yes, then, what are the traits or characteristics that make an algorithm ethical?

As algorithms, machines and technological systems are incorporated into different areas of life, as data has become more and more indicative, as great amount of data collected and made sense for different purposes, there are new emerging fields and new challenges posed by algorithms. We are seeing the benefits of algorithms/machines working with increased autonomy or we are seeing them with learning and decision-making features creating value-laden results, but we want to figure out how to make them act ethically (Allen, Wallach & Smit, 2006, p. 15). Before developing ideas on how to make algorithms ethical, it is first necessary to ask if it is possible to study ethics of algorithms. That is to say, is it possible for machines to be moral and act ethically? Which agents can be ethical? Can an algorithm be moral and carry specifications to be regarded as a moral agent?

First of all, what is a moral agent? According to James Moor, there are four types of moral agency: ethical-impact agents, implicit ethical agents, explicit ethical agents and full ethical agents (Moor, 2006, p. 19-20). With the conceptualization of Ryan Tonkens, explicit ethical agents and full ethical agents will be taken into examination which are found relevant for the purpose of this study (2012, p. 139). Explicit ethical agents are the ones which would be able to make judgements and justify them ethically and also which can “handle real-life situations involving an unpredictable sequence of events” while acting out autonomously (Moor, 2016, p. 20). A full ethical agent is considered as an "average adult human" which would be expected to have "consciousness, intentionality, free will" (ibid) and also "creativity and emotions" (Tonkens, 2012, p. 139) like humans do. However, no artifact has reached that point.

Is it possible to create full ethical agents or even explicit ethical agents? What does moral judgement require to be moral? What are the traits? Allen et al. asks "does moral judgement require consciousness, a sense of self, an understanding of the semantic content of symbols and language, or emotions" (2006, p. 14)? Even though, they leave the question open to developments and suggestions in their paper, they suggest that moral agency is thought to be a sentient being with the trait of free will, according to philosophical and legal concept (ibid). Similarly, Tonkens suggest that for artifacts to be moral (full or explicit), they need to be "conscious rational, autonomous and possess at least some (proto-) emotions" (2012, p. 142). Furthermore, Anderson & Anderson questions if machines are kind of entities which can act ethically (2007, p. 19). They emphasize that in order to be a moral agent, an entity needs to be able to act intentionally which requires that agent to be conscious and to have free will (ibid). As a result, the characteristics/traits for an artifact to be a moral agent can be concluded as being a sentient being with free will, consciousness, rational thinking autonomy, (proto-) emotions and intentionality. The concern about whether an agent can behave ethically or not stems from the dilemma if artifacts are capable of aforementioned traits and characteristics. This is because being an ethical agent comes with *moral responsibility*. Can an artifact be responsible for its unethical actions? If not, can we really talk about intentionality of the artifacts?

There are two main approaches to moral responsibility: 'classical approach' implying that responsibility cannot be ascribed to artifacts and 'pragmatic approach' implying that *artifactual (functional) responsibility* can be ascribed at various degrees to artifacts (Dodig Crnkovic & Çürüklü, 2012, p. 64). The logic which discusses that we cannot ascribe moral responsibility to artifacts holds the idea that it is meaningless to assign blame, praise, punishment or reward to the artifact, if it is not able to understand the consequence of its own actions (Floridi & Sanders, 2004, p. 366; Dodig Crnkovic & Çürüklü, 2012, p. 64-65). According to Nissenbaum (1994), two conditions should be considered to evaluate whether the agent is morally responsible for its actions or not: causal responsibility which is already discussed above and mental state which is discussed with intentionality of the agent (p. 74). The argument that artifacts lack of mental condition like intentionality can be discussed that intentionality is an observed behavior; we do not know the inner workings of human mind, while we know more about the inner workings of a computer system (Coeckelbergh, 2010; Dodig Crnkovic 2006 as cited in Dodig Crnkovic & Çürüklü, 2012, p. 65). It is obvious that artifacts do not have the same sense of intentionality in their actions as humans do, but their learning capacities and improvements will make it possible to assign them artificial responsibility or agency which will fulfill the two states 'causal responsibility and mental state', but for now what we can adopt is "*moral responsibility as a regulatory mechanism"*[51] (ibid). And this is not related to making the artifact responsible for blame or praise, but it is related to assuring ethically appropriate behavior for the agent (ibid).

As a result, it is time to answer why and how artifacts can be ethical agents and why the thesis considers algorithms as ethical agents and ethically responsible for their actions. The idea why we think that we have reasons to think algorithms as a subject of ethical scrutiny and why it is a valid idea has three foundations. First, according to Verbeek, ascribing some morality to artifacts is plausible (2008, p. 91), because artifacts are active in the sense that they shape human actions, decisions or interpretations and their lack of consciousness does not mean that they do not have intentions, and the intention of the artifact is understood in the sense of *directing* (ibid, p. 95). Their mediating capacity ascribes them some kind of intentionality. However, this intentionality does not occur on its own (from the algorithm itself) or it does not derive from the human, but it emerges in relations between humans and artifacts, so it can be called 'hybrid intentionality or distributed intentionality' (ibid, p. 96). So, the morality is understood as a mixture of the human and technology. Also, according to Anderson and Anderson, neither of these traits is needed to act moral in ethical problems and to justify the action (2007, p. 19). What is needed is that algorithm acting in a way which is deemed morally correct for that particular situation and being able to justify the action with an appropriate ethical principle that it has followed (S.L. Anderson, 1995 as cited in Anderson & Anderson, 2007, p. 19). So, if algorithms/machines are regulating,

[51] Emphasis is added.

directing and creating value-laden outcomes, it will be wise not to stick around the discussion on intentionality or consciousness, but rather focus on the action of the machine and think if it is morally acceptable. The third perspective is that we can hold algorithms accountable for their actions and they can be a subject for ethical discussions, because "agents with morally significant behavior should have moral responsibility" (Dodig Crnkovic & Çürüklü, 2012, p. 64), but if only they are regarded as parts of a bigger socio-technological organization which means that responsibilities of the artifacts are distributed and networked in those complex systems, and giving some degree of responsibility to agent has actually a regulatory role (ibid, p. 65). That is to say, it is essential to attribute agents some *functional moral responsibility* (ibid, p. 66) to understand their regulatory role in complex networked systems where roles are distributed.

Having discussed morality of artifacts, moral responsibility of agents, traits/characteristics of moral agents, we will now focus on the questions: why are ethics of algorithms discussed, what are the unethical practices / problems and how are they discussed? Ethics of algorithms are discussed, because they are systems which fulfill tasks, learn from data sets, make automated decisions and create value which has moral consequences in various fields ranging from employment, crime prevention to education and economy. According to Ananny, algorithms raise ethical concerns when they "signal certainty, discourage alternative explorations and create coherence among disparate objects –categorically narrowing the set of socially acceptable answers to the question of what ought to be done" (2016, p. 103). In other words, we discuss ethics of algorithms, because we would want the systems that we create to be sensitive to our understanding, values and morals with their governing capacity, deciding the "ethical acceptability of the options they face" (Allen et al., 2006, p. 14). This means that we would not want to take away the value-laden capacities of algorithms from them to make them behave more ethically, but we would want these capacities to be actively performing when any ethical consideration is needed.

When ethical algorithms come into question, it is important to underline that what is discussed is not the algorithm itself, but the discussion is oriented to find out why algorithms works in that specific direction or why it creates that specific result. For example, if Google's algorithm autocompletes the sentence "why Americans are so…" with 'fake' or 'extra', the idea should not be to put blame on the algorithm itself, but the effort should be to understand why algorithm created that result. Besides, the question 'what does it mean for an algorithm to be ethical' is often related to *neutrality* of the algorithmic systems. Algorithms are often thought to be neutral entities which produce unbiased and better outcomes which can result in better ethical practices. Algorithms are expected to produce better results than humans as they are thought to be lacking of human prejudices, bias and discrimination –more generally, human touch. However, algorithm is not neutral, because there are effects of an engineer who designs the system and also data sets can lead to non-neutral results. As algorithmic systems are regarded as not having emotions like humans do, they are believed to produce better ethical results. While emotions were thought to be dangerous and misleading for algorithmic systems to produce non-neutral results, the perspective has changed today. In fact, emotions are considered as key for ethical rational behavior and emotions help to learn from mistakes and help to orient right virtues, feelings and sentiments (Damasio, 1994; Allen et al., 2006, p. 16). On the other hand, there are times when machines/artifacts will be better in behaving ethically or making ethical decisions. While human beings may have a tendency for unethical behavior for their survival as being biological entities, artifacts lacking this predisposition may actually be better in ethical behavior and even inspire human beings to be more ethical in that sense (Dietrich, 2006 as cited in Anderson & Anderson, 2007, p. 17). As a result, it was believed that neutrality will give more objective and ethical results, but algorithms are far from being neutral and this will be explained with unethical practices of algorithms. Besides, according to Ben Wagner (2016), technology is not neutral, good or evil, but it reflects power structures which impact human life (p. 11). In other words, algorithmic systems are not free from the power structures of the society, they are responsive to that.

Therefore, looking at the ethical problems posed by algorithms is essential to understand what kind of struggles and power structures exist. Tüfekçi et al. defines three attributes which make algorithms 'a new category of concern' and they describe them as "opacity/complexity, gatekeeping and subjective decision-making" (2015, p. 3-6). These are considered as traits to explain how algorithms are now creating value-laden results which impacts social life. They also develop responses to make these systems more ethical and they suggest ‘transparency/notification, algorithmic accountability and government regulation of algorithms’ (ibid, p. 11-12). The discussion around ethics of algorithm mainly focuses on discrimination, bias, justice, automation, ossification, manipulation, power asymmetry, eco chambers, filter bubbles, fairness, appetite of consumption, data ownership, narrowing of world views and lessening of social encounters. Ethics of algorithms is also discussed with *disparate impact* which is the adverse effect of the algorithmic system to produce unfavorable results while the system had no intention to do it; it happens to particular groups on the basis of status, gender, age or disability. Jagadish exemplify disparate impact as distributional unfairness, ossification, surveillance and asymmetry (2016). These are mainly seen in hiring, recommending, scoring and predicting algorithms which take gender, age, status or other *life data* into consideration.

When people come across with these problems, it is important to figure out who is considered as accountable or responsible for the actions and decisions of the algorithms. Is it the algorithm itself? Is it the designer or engineer? Is the data set? Is it the platform or the company? And, is there any responsibility assigned to the users?

According to *Engineering Ethics*, designer or engineer is responsible for what s/he creates (Dodig Crnkovic & Çürüklü, 2012, p. 62). This may include the design, implementation and possible (negative) outcomes. And, this idea requires engineers to have a *full* control of their creation, the whole system and the procedure. However, it is important to realize that morality implicit in an agent is not the only concern of the engineer, because it is not always possible for engineers to predict the outcomes or to foresee how a technological system will act in a complex structure (Allen et al., 2006, p. 13). When many engineers contribute to the design and implementation of the algorithmic systems, no single person can fully understand how a system will interact or respond to new inputs (ibid, p. 14). Therefore, it can be concluded that engineers are expected to share responsibility for their art, but there should be a distributed responsibility when there are many people finalizing a technological system. So, engineers can take a sense of responsibility and a distributed accountability, but they may not have a full control of their creations.

On the other hand, *Machine Ethics* tries to compute ethics into machines to create a moral agent which is able to evaluate the best ethical practice and to justify its actions. Machine ethics perspective claims that embedding ethics into machines is required for machines to be autonomous in accordance with ethical standards (Dodig Crnkovic & Çürüklü, 2012, p. 62) so that it can create ethically desired results. Thus, the responsibility for ethical behavior is ensured by coding ethical understanding of social life into the systems. However, it is important to think about how an engineer can code ethics into a system which is unstable and which has capacities of learning and changing. As discussed by computer engineers, it may not be always easy or possible to code ethics into algorithms and to receive ethical results after a certain period of time. Thus, different variables need to be taken into consideration when assigning responsibility to an engineer to code ethics and when expecting machine agent to create ethical results.

The approach which holds algorithm itself responsible or accountable for its actions signifies an important shift which takes responsibility away from the human being and assigns it to algorithm. This shift assumes that algorithm's assessment is more effective than assessment of human beings who develop the algorithm (Wagner, 2016, p. 7). This shift also attributes adjectives to algorithms which actually pertain to human beings such as racist, discriminative, biased and etc., drawing attention to the fact that algorithms gain agency and autonomy at some degree. Malte Ziewitz discusses that attributing power relations or control to algorithms and engaging politics or governance with algorithm is creating an "algorithmic drama" which cannot even describe what an algorithm is, but holds it responsible for the emerging social problems (2016, p. 4-5) Similarly, Daniel Neyland criticizes the literature for discussing algorithms as creepy entities which are out of control, independent, inapprehensible and calls it a compelling drama (2016, p. 51). Kate Crawford also states that there is a persistent problem of fetishization of algorithms (2016, p. 89). The conceptualization here is that algorithm is just an algorithm. The idea that algorithms are accountable for themselves is challenged. Algorithm does not happen by itself or it does not work on its own, but they are related to people who use, implement and design them. They are not stable, but they are moving entities.

Therefore, one approach to algorithmic accountability focuses on the human touch effect where the decisions of the engineers in the design of the technological systems play an important role. The idea is that ethical perception, world view, morals and values of the creators affect how an algorithm will work and what kinds of results it will produce, because ethical standpoint of the designer is a part of the process, contributing consciously or unconsciously. This literature focuses on design justice (Costanza-Chock, 2018) and flourishes from the ideas that algorithms are non-neutral and practices can cause harm. However, it is important to notice that these considerations are different from the drama literature which blindly fetishizes algorithms.

Another perspective to algorithmic accountability focuses on data set for biased outcomes, instead of the algorithm itself. Algorithm has a simple definition and the reason why it is associated with so many social impacts and why it creates complex issues which are cohesive with today may stem from the fact that the answer is actually not the algorithm, but the data set algorithm works on. It is discussed that more inclusive and diverse data sets will result in more ethical outcomes. In this way, algorithm can have the opportunity to come across with different examples and to learn from diversity. As a result, it can identify patterns diversely and come up with better decisions.

A different perspective assigns responsibility to users. Kraemer, Overveld and Peterson discusses that designer should design algorithmic systems in a flexible way which is open to meeting the requirements of different ethical situations (2011, p. 259). They propose that algorithmic systems should be open to ethical preferences of the users, meaning that transparency over designer's choices is not enough, but users' own control over the situations is needed so that s/he can situate herself/himself in different ethical settings (ibid). This means that transparency over decisions of the designer does not empower the users. However, designing algorithmic systems in a way which allows users to choose ethical factors is a real solution and makes users gain agency. Also, Lokhorst state that transparency over designer's choices enables to know who is responsible for what in a technological system (Lokhorst, as cited in Kraemer et al., ibid.). This can be a solution for the 'many hands' problem of technological systems, by knowing who contributed to which process. However, Kraemer et al. (2011), discusses that transparency is not empowering for the users, so designer should give the responsibility of defining the defaults of the software to user herself/himself (ibid). In this way, users gain agency, they are empowered to define their own default settings and they are hold responsible for the potential outcomes. At this point, it is important to consider Ananny's question: "should users be held partly accountable for an algorithm's output if they knowingly provided it with data" (2016, p. 109)? This question is a good one to think about the accountability assigned to users. If users have the choice to regulate their default settings of the system for better ethical results, then the answer is believed to be yes. However, if users are not allowed to make decisions in the system, then the answer is believed to be no, even if users provide the system with data knowingly.

The perspective of this thesis study to responsibility and algorithmic accountability is that it would not be healthy to adopt a reductive approach. The first idea upheld is that there should be a distributed and networked responsibility and accountability, because there is not a single area of responsibility and there are many people contributing to different parts and processes of these socio-technological assemblages. The second idea is that even if the designer code ethics into algorithmic system, algorithms are changed by designer multiple times and algorithms are changing structures with their learning capacity. Therefore, the idea questioning the sustainability of ethics in an unstable basis sounds quite reasonable. The third idea is that economy politics always matters. The responsibility of platforms and companies is an important one to scrutinize, because they will try to implement what they make money off and what will bring the most profit. As Safiya Noble discusses, they will say "we are sorry if we offended anyone, we are working on it" and try to adjust their systems, only when they get reaction from the society (2017). It would be disingenuous to say that companies/platforms are not implicated, because they will always try to propagate what they make money from first (ibid). Therefore, this study is of the opinion that platforms/companies should undertake a bigger slice from the responsibility issue. The forth idea is that people who develop and design technology do not aim to harm society or hurt people. It would be wrong to consider these people as evil, whenever society is affected by outcomes of their technological advances. However, Safiya Noble discusses that a person cannot design a technology for society, if s/he does not know the society itself and it is a wrong direction to center the technology, instead of recentering the people (ibid). That is to say, she states that "those who know so little about society [should] have no business designing and deploying their technologies on society" (Bulut, 2018, p. 296). What is discussed here is that technologists need to think about the social impact of their developments on the society, but they can only do this if they know the values, problems and Geist of the society. Only then they can develop a technology for society, because they will then know and foresee the risks of their work. And in terms responsibility, focusing on people instead of the technology itself is found to be cohesive for this study. The fifth idea is that socio-technological assemblages are interactive, changing and learning systems. Therefore, in order to obtain ethical results, there is a responsibility for everyone in the socio-technological assemblage –designer, platform, users, data-set and the algorithm. Because it is algorithm, data and human assemblage, as much as we create technology, it also comes to shape our space, life and the way we do things.

2.1.4. What is the ethical approach of this study?

Finding the *right* ethical approach for this study means being able to answer *how* people can embed idea of human life, understanding of social life and meaning of values into algorithms, data and code (Pariser, 2011b). However, there is not a single *right* answer to this question in this thesis. It is rather a combination of different ethical perspectives which are only then believed to be able to bring insights on the solution of ethical problems. This is simply because there is no single ethical perspective in the literature that could have been a solution for all the ethical problems rising from the features of algorithms and related practices.

However, it is important to look at the studies which adopted deontological, teleological and virtue ethics approaches to create moral AMAs (artificial moral agents) or machines, because this discussion is considered as constituting the basis of the discussions around the ethical algorithms. According to Wallach and Allen (2009), virtue ethics is a promising moral framework to create autonomous AMAs possessing ethical actions (as cited in Tonkens, 2012, p. 137). Virtue ethics approach is found to be helpful for containing both top-down and bottom-up approaches and that hybrid computational approach is promising and necessary to embed ethics into AMAs in terms of *computability* compared to deontological or teleological approaches (Wallach & Allen, 2009, p. 117-119 as cited in Tonkens, 2012, p. 138; Lin et al. 2008). Tonkens discusses it should be ensured that creators behave morally when they create and use machines or AMAs and that ethical consideration should come before the creation of the machines (2012, p. 148)[52]. According to Anderson and Anderson, best approach for ethical theories is the one combining both teleological and deontological elements (2007, p. 18). And for this, they adopt the prima facie duty approach which they consider as better than absolute duty approaches at revealing complexity in ethical decision making (ibid, p. 22). Because they believe that prima facie duty approach not only includes good elements of teleological and deontological approaches into ethics, but it also allows for necessary exceptions to adopt other approaches and it is better at adapting to different ethical dilemmas at different areas such as legal ethics, journalistic ethics and etc. (ibid, 22). *Traditional* ethical approaches questioning the morality of the AMAs are good to teach ethical thinking and to constitute the basis of the structure. However, adopting these approaches or selecting a single approach to study ethics of algorithms is not enough or possible because of six complex reasons that are previously mentioned: distributed and networked power relations, concept of agency, knock-on effects, problem of knowable outcomes, unstable nature of algorithms and many hands problem. It is believed these problems cannot be solved only by defining ethical principles to implement or by specifying a particular ethical approach to systems.

As a result of this, there are more current and comprehensive researches which adopted different ethical approaches to study and implement ethics into algorithms in terms of new emerging problems[53]. Also, it is believed that tendency to study ethics should not be about naming a particular approach, but it should rather be about questions that are directed to define necessary ethical considerations for the emerging problems. For instance, Neyland develops ethnographic approach aiming to develop algorithmic

---

[52] He argues that before creators focus on the computability of Machine Ethics, the ethics of Machine Ethics should be included into ethical considerations (2012, p. 141). And, there should be compatibility between moral framework, moral standing and tenets of moral framework: that is to say, if compatibility is not ensured, it means that creators are asking AMAs to behave against the moral instructions they design for the machines to follow (ibid, p. 140).

[53] This does not mean that thinking on *traditional ethics* is not helpful to study ethics of algorithms. It rather signifies the urge, importance and need to build on these ethical considerations which will be able to understand the problems of today.

accountability and to study ethical algorithms for spaces like airports or train stations (2016, p. 53-54) and he benefits from ideas of ethnomethodology. Annika Ricterich adopts pragmatic approach to study ethics suggesting that pragmatic ethics “accommodate epistemological insights into the fallibility of (scientific) knowledge, while allowing for critical assessments of societal power structures” (2018, p. 24). It is found as a strong point to study ethics in a technological culture.

However, there are some current and comprehensive ethical perspectives that are found *suitable* for the purpose of this study. One ethical approach that is deemed suitable for the purpose of the thesis comes from the literature of H. V. Jagadish. He discusses that data science needs code of conducts, but “regulation is not the answer”, because while technology develops quickly, regulations are enforced slowly (Jagadish, 2016). It is good to have regulations or law to follow discussions that have already been issues of societal consensus, but it requires too much time for any moral value to become law or regulation (ibid). Therefore, it is not practical to wait for regulations and laws to regulate data science. However, ethical thinking is practical. For example, as in the case of GDPR, it took years to replace Data Protection Directive and it also took two years for it to be implemented. Therefore, what Jagadish is telling that it is easier and quicker for actors in a technological assemblage to adopt ethical perspective, instead of waiting regulations and laws to enforce ethical practices. For this, he offers two starting points: the first point is that “do not surprise the subject of data” which requires asking “who owns the data, what can the data be used for” and “what can you hide in exposed data” (2016). And the criterion of not surprising the data subject is based on how most people think, behave and act generally: the criterion is about following the societal consensus[54]. The second point is “own the outcomes” which requires asking “is data analysis valid, is the data analysis fair” and “what are the societal consequences” (ibid). The criterion of owning the outcomes is based on the need to understand the outcomes, intent of the laws, the logic of the regulation and the ethical position of the societal consensus.

[54] It is important to mention that ethics is responsive to culture and society. Societal consensus will be different in every society, because what members of the society think and value will be different. For example, protection of privacy may have more importance in European societies than American societies. Thus, invasion of privacy can be more common and can be more generally accepted in American societies as a natural consequence. Because, the societal consensus -the general idea- on data protection will have different values and will be accepted and practiced differently.

Another ethical consideration the thesis finds suitable is the study of Ladikas, Chaturvedi, Zhao and Stemerding (2015). What this thesis study adopts from their research is their considerations on ethics and culture. The first is that cultural norms affect values of the society and ethics do not come into existence out of a void and ethical discussions cannot be separated from cultural norms and values (2015, p. 3). The second is that ethical debates are policy debates and ethical opinions are policy opinions and ethics aim to affect policy-making (ibid, p. 3-4). However, embedding ethics into policy-making also does not happen on its own, it is not a stand-alone concept, but it is connected to culture affecting various aspects such as values or history (ibid, 4)[55]. This idea that ethics is inextricably bound to culture and that ethical opinions form the basis of policies is found to be quite compatible with the purpose of the thesis.

A different ethical approach the thesis adopts is *impact model of ethics* developed by Annette N. Markham where the attention is given to possible future directions (2018, p. 7). Impact model acknowledge that while it is useful to clarify object of the study, characteristics of data and characteristics of people, impact model considers these kinds of decision-making as processes which emerge in bigger systems of actions, through longer time spans (ibid). This model situates a lens at a future point so that one person can look back to understand why and how a specific effect might have happened (ibid), it is a similar understanding of reverse engineering that is applied to ethical thinking which is found quite helpful for the ethical approach of the thesis. This model has anticipatory function which is useful for "large scale analytics, experimental research, or technology design environments when the ethical problem is not apparent in the immediate moment but can be seen through speculative lens" (ibid), helping to understand possible outcomes and to realize pitfalls of the current systems. So, the impact model aims possible impacts, rather than preventing the impact first (Markham, 2016). Markham separates impact model into four different arenas.

The first arena is *treatment of people* which builds on psychological and sociological disciplines where the center is on human rights (Markham, 2018, p. 8) This arena

[55] One interesting question that can be directed here is that what would be the ethical perspective of big global companies such as Facebook, if understanding of ethics changes from one society to another? This question can also explain why different societies have different reactions to privacy breaches of Facebook.

assumes that developers / researchers interact with their subject (human / non-human) and it looks into impacts on the subjects, for instance by asking the possible impact of manipulation of user's environment in order to test inputs of a system (ibid). The second arena is *side effects* which builds on science and engineering disciplines and assumes that unintended outcomes are natural in research or technology, but the precautionary principle helps to evaluate the effects of science (ibid). Side effects can be caused by a research or diverse factors in the platforms which makes assigning the responsibility to a specific person difficult (ibid). For example, it asks how design or implementation of technology impact people in unexpected ways (ibid). The third arena is *use of data* which builds on cultural studies, critical and feminist studies and disciplines where the center is on politics of power and marginalization (ibid). This arena focuses on how data are used by different partners for different purposes, it considers how analytics create generalizations about people, consolidating or challenging social categories (ibid). It may ask how data aggregation or data analytics avoid some basic rights (ibid). The forth arena is *future making* which builds on speculative domains, assuming that all research or any development small or big will impact future cultural / social formation and it may ask questions such as what is the possible impact if some specific trends on technological development became permanent units in society (ibid, p. 8-9)? As a result, the impact model is found as a suitable approach to study ethics, because it focuses on the potential outcomes of a technology by thinking on the potential impacts of the technology created. Also, it is comprehensive in understanding technology as social and technological assemblage by providing ethical insights about treatment of people, use of data, side effects and future course. Moreover, while it pays attention to legal context (such as law, regulation etc.), it also considers responsibility in terms of morals; it prefers not to focus on the ethical guidelines too much to sustain ethical systems, but it focuses on morals as regulations which is the main perspective of the thesis.

Finally, the ethical approach of this thesis is that there is not a single ethical perspective that can be the remedy for all the problems users, developers and technologists face. The solution can be *not* adopting and focusing on a single ethical thinking. Not specifying a specific approach does not mean taking the easy way out of the problem, it realistically shows that there is no standard of the ethical problems and there cannot be a standard approach to adopt, because problems are various[56]. Therefore, ethics of social and technological assemblages require practicing ethics as morals and combining different perspective for various situations. Also, it is believed that embedding ethics into assemblages needs to be compatible with how a person thinks and what a person tells an assemblage what to do. Moreover, as discussed by Ananny, "in reality, technology ethics emerges from a mix of institutionalized codes, professional cultures, technological capabilities, social practices, and individual decision making" (2016, p. 96). Therefore, it is important to think that ethics do not happen out of a void, ethics cannot be implemented simply through guidelines, ethics cannot be embedded into technology simply by following dos and don'ts, it requires culture, social practice, individual responsibility in the forms of morals and decision-making as much as it needs codes of conduct, regulations, reflections on the outcomes of technologies and considerations on the design and practice.

It is believed that finding the right approach to study ethics of data-driven algorithms is only possible by understanding the impacts of these socio-technological assemblages. However, in order to achieve this, it is necessary to understand that questions raised by technology emerge with *rapid* developments which require studying ethics *now*. The next question aims to provide insights in respect to this.

2.1.5. Why is it important to study data ethics now?

Data-driven algorithms need ethics. It is because algorithms working behind programs and machines are not cold assets which are far away from social life. On the contrary, they are procedures which have great social consequences and impacts. And "ethics [provides and suggests] us a better way of doing something in so many aspects of society" (Jagadish, 2016). And, it is believed that there are complex issues which urge studying data ethics *now* and this part of the thesis aims to reveal the reasons why starting a discussion on data ethics matters.

---

[56]For example, it is discussed that for more inclusive algorithmic results, data sets should be more diverse. However, it is important to realize that there is no standard ethical requirement for diversity as discussed by Amy Webb. Also, there is no standard design justice requirement. When this is the case, ethical perspectives do not have a standard point to adopt, but it is rather a more comprehensive and inclusive combination of different solutions (Rainie & Anderson, 2017).

It is important to study data ethics *now* because of four reasons. The first one is that we are currently living in a world which has never been this much data-driven before. As algorithms are deployed in more areas of daily life, people are also seeing their impact more in so many parts of their lives. And, in modern information societies, we are producing so much data, because most of our lives are digitalized. And, data which are great story tellers are able to give away many details of one’s life (even the private ones). As a result, value is extracted from the data, because data provide insights about one person’s geographics, demographics and psychographics such as social life, economic status, culture, habits, preferences, location, age, gender etc. This makes data the main input of the economy and makes production (processes) to be based on data in information societies. As a result of this, every process and eventually our works are based on data. It is believed this will increase in the future. Not only because more and more parts of our lives are digitalized or data-driven, but also because of the fact that these digitalized devices will be communicating with each other more and more via sensors. So, there is more efficiency waiting us in the near future. And if we do not take an action now, it will be no surprise that we will go through a digital revolution where we will be abused incredibly. To sum up, as abundance, capacity and possibilities of data increases, it is essential to discuss the ethics of it to understand the society we live in, to figure out where this society leads to and also to gain more control of our lives.

The second reason stems from the fact that we are experiencing more and more ethical problems about data than ever before. As data are deployed more and become more visible, it also becomes a topic that society needs to have a social consensus which is built on societal values. As the discussion surrounding the data science ethics is relatively new and as it is not discussed at length, there are not enough social consensuses on the ethics of data regarding their effects and impacts at societal level. And, it is believed that this is the reason why we cannot have a common understanding of data ethics. Therefore, it is important to discuss it in order to create shared social values which will lead to ethics in the end. It is because ethics are based on social consensus, they are not law, they do not have legal enforcements, but they prepare the basis of the legal actions. To sum up, there is not a social consensus about data ethics yet (because it is not discussed enough). However, after the discussions surrounding data ethics gain recognition and visibility, it is believed that the society will come close to a social consensus eventually.

The third reason why we should be discussing ethics now is that technology is developing fast and sometimes regulations are enforced slowly. It is not always possible for regulatory actions to catch up with the speed of innovation in a timely manner, and because of that the regulations sometimes become irrelevant. It is also possible that companies or third parties will be done with exploiting the user data, until a regulation comes to help. As a result, it can be concluded that regulations can take time, but ethics can be practiced much faster (Jagadish, 2016).

The forth reason is that if data ethics is not discussed now, it is highly possible that the field will be closed to discussions. It is because of the fact that there are many decision-makers, companies, third parties and institutions which want to deploy and use algorithms for their profit and interests. There are many actors who do not think about the ethics, privacy and power asymmetry. In a social system where powerful agents (which have the power to collect, mine and process data) are able to reach every aspect of a person's life, it will be hard to control the actions of the agents without ethics. It is because no government and no company would like to refuse making use of the capacities of data for their business and endeavors; none of them can say “no” to such a great power which can give them control over citizens and customers. As a result, if the field stabilizes without discussing the ethics, this means that the field will be ossified and the social consensus will be set in that direction. That is to say, it will be normal for citizens that their data will be exploited, commodified, sold, collected and processed without their consent. Therefore, it is important to understand that an ethical discussion opens the field and provides it with necessary critics. It will also challenge agents to be fair, ethical, responsible and accountable for their actions. To conclude, if there are no challenging discussions on the field, it will mean stabilization of the unethical, ossification of the problems and closure of the discussions in data science ethics.

2.2. ETHICAL PROBLEMS RISING FROM FEATURES OF ALGORITHMS AND RELATED PRACTICES

This section of the study aims to provide a structure for the discussions surrounding data-driven algorithms. For this, an ethics map is created. The map does not have the aim to suggest ethical solutions to the problems, but it aims to build a framework for the ethics discussion addressing the problems in the field, features of the algorithms and types of the algorithms. Some of them (both types of the algorithms and rising problems) are discussed in the first chapter. However, they are not discussed within the framework of ethics. Therefore, it is believed that previously discussed parts should also be placed in this map. This section of the study aims to provide real examples emerged from data-driven algorithms and related practices on algorithms and data.

2.2.1. An ethics map for the data-driven algorithmic discussions

	Ethics Map	
Problems rising from data-driven algorithms and related practices	**Features of Algorithms**	**Types of Algorithms**
Invasion of Privacy	Decision-making	Personalization
Discrimination	Autonomous	Recommending
Bias	Learning	Ranking
Automation	Prioritizing	Machine Learning
Ossification	Micro-targeting	Predicting
Manipulation	Opacity	Targeting
Asymmetry	Gate keeping	Tracking
Data ownership		Scoring
Commercialization		Filtering
Consumerism		Profiling
Appetite of Consumption		

Table 1: Ethics map

The ethics map aims to cover societal impacts of the algorithms. It argues that different types of algorithms cause different ethical problems with their distinctive features which are listed above –but not limited to this-. It is important to mention that there is no direct correlation between ethical problems and features and types of algorithms in this map. That is to say, there is no “single axis” (Floridi & Taddeo, 2016, p. 4). For example, opacity feature of algorithms may cause asymmetry of power, but it can also lead to invasion of privacy in different cases. The main aim of this table is to discuss the ethical problems in-depth by covering the literature on that ethical concern instead of arguing it in a definitional way. That is to say, instead of asking what discrimination is, the map aims to ask why and how discrimination occurs as an ethical problem due to data-driven algorithms and how it is discussed in the literature. Besides, each ethical problem will be discussed with case studies aiming to provide real examples emerged from data-driven algorithms or related practices of the parties on data and algorithms. The examples are selected on the basis that they emerged on OSPs. Some other current examples that do not take place on OSPs will be discussed in footnotes, as they are considered as eye-opening. In this way, it is believed that problems and the discussions will be more concrete and not understood as just technological constraints, but real-life experiences that people encounter every day. To sum up, the ethics map will be fed with academic discussions surrounding ethical problems and it will be empirically supported with case studies.

2.2.1.1. Ossification

Ossification is the conceptualization of H.V. Jagadish in his online course Data Science Ethics which is discussed as parts of disparate impact of algorithms. The reason why this conceptualization is found suitable for the ethics map is that it can explain social impacts of eco chambers and filter bubbles such as reinforcement of opinions, beliefs and consolidation of stereotypes on social networks.

Ossification is defined as “the tendency of algorithmic methods to learn and codify the current state of the world and thereby make it harder to change” (Jagadish, 2016) which means that algorithms are systems and procedures which aim to “maintain the status quo” (ibid), and that it may strengthen the patterns in the dataset by learning and codifying, making it harder to change. For example, it was previously discussed that people are selective of their relationships and choices, they have conscious and unconscious biases and prejudices and they tend to communicate and interact with people that is more similar to them in offline world. But the decisions of talking, listening to or interacting with someone belong to the person. S/he has the chance to come across with counter ideas which is important for the development of public structure. However, the ethical problem with social networks is that they are automatically selecting, omitting and curating what to see, who to listen, who to read, with whom to interact with their algorithms working behind to give the most relevant content to their users which was discussed as eco chambers and filter bubbles in the first chapter[57]. This is resulting in missing out of conflicting opinions, narrowing of world views, consolidation of stereotypes, or "reaffirmation of preconceived notions", because these things "get baked into algorithms" (ibid) which results in ossification of these prejudices, biases and judgements algorithmically[58].

In order to challenge and burst filter bubbles and eco chambers, two people have tried something experimental. One of them tried to game the systems by liking everything for two days on Facebook and the other one tried quitting liking things on Facebook for two weeks, independent of each other. When stopped liking posts on FB, it is noted the stream has become "more akin to eclectic dinner party" (Morgan, 2014) and the person who experienced this game reports that it felt like less connected, but there was more conversation, as she was communicating with comments, instead of likes (ibid). The overall result was that she was getting "more of what [she] actually wants rather than just being served more extreme versions of what [she] likes" (ibid). On the other hand, the other person gamed the system and liked everything that Facebook sent for two

---

[57] It is discussed that *filtering* algorithms are causing eco chambers and filter bubbles. Filtering consist of "including or excluding information according to various rules or criteria" and "filtering decisions exert their power by either over-emphasizing or censoring certain information" (Diakopoulos, 2015, p. 402). Thus, filtering algorithm is one the determinant of which information to be presented to users.

[58] The main reason for missing out conflicting posts of friends or not seeing irrelevant content on the newsfeed is actually because *personalization* algorithm that is working on the platform. It was previously discussed in the first chapter of the study that personalization algorithms tailor information based on user's interest and online behavior. And, Facebook's personalization algorithm "prioritises content based on the date of publication, frequency of interaction between author and reader, media type, and other dimensions" (Mittelstadt et al., 2016, p. 10), resulting in narrowing of world views.

days. The important result was that liking anything that is on FB turned newsfeed into a new character and it "became about brands and messaging, rather than human with messages" (Honan, 2014). The newsfeed filled with notification from brands and politics as the interaction increases and also FB reported the person's activities to his friends and followers (ibid). That is to say, not only his newsfeed, but also other people's feeds were affected by his "weirdo activity" by "overrunning their feeds" (ibid). Therefore, not liking stuff *may* help people to break the filter bubbles and liking everything may make filter bubbles more commercialized and eco chambers more politically filled, but it may not make sense at all for the person who was trying to game the system, as it becomes politically less relevant. It can create non-sense and messiness, too.

The ethical implication is that algorithms can reinforce current status quo such as maintaining a person's newsfeed with like-minded people's posts, shares and likes. People may struggle to burst their filter bubbles, as they are trapped into a commercial loop of relevancy. In other words, homophily can be an instrument for companies to make people spend longer times on their services by providing comfort and enthusiasm of hanging out with likeminded people. This may cause narrowing of world views and social encounters, breaking down of public structure and missing out confronting world views thanks to personalization algorithms.

2.2.1.2. Invasion of Privacy

Privacy is discussed with different concepts such as informational privacy, right to be forgotten, right to privacy, personal and public data, group and personal privacy, data protection, control and access to data, identification, anonymity and etc. Different cases will be discussed to examine how privacy is invaded and which moral problems it reveals.

The first case to be analyzed for invasion of privacy fits in the framework of *dataveillance*. However, definition of dataveillance and how it happens were discussed comprehensively in the first chapter. Therefore, it is now time to look at the ethical implications of it and understand how and why it becomes a part of ethical discussion.

The following case study is about *mass dataveillance* which is described as “the systematic use of personal data systems in the investigation or monitoring of the actions or communications of groups of people” (Clarke, 2016). And, one of the areas it is increasingly used nowadays is to surveil social movements and protests by monitoring social networks.

Over the years, social media and networks have been powerful tools for people, activists or journalists to communicate, to organize, to express and to be heard of. Social networks provide media coverage for dissidents; social media has become medium for activism in the recent years; protestors get organized on the platforms during social movements or protests. And in a social movement that is coordinated and communicated on social media, thousands of Tweets containing text, video and images are shared, locations are provided to inform what is happening where, announcements are made to organize next plan of the movement. All this information about the protests or people’s own actions can come at high price, when they are used by governments or police departments to undermine. The empowering platforms can be turned into dataveillance/surveillance mechanism to profile protestors and they can be further used to map the course of the protests.

In authoritarian regimes, the posts of activists can put them in vulnerable positions, as they are not only aggregated to build a picture of user’s likes, tastes, preferences but also political views, personal beliefs and details (Al-Sharif, 2018). It was rumored that Gulf Cooperation Council governments decided to use activists’ old tweets to create cases against them (ibid). As a result of this fear, many activists took measures to delete their previous tweets (ibid). In the meantime, Twitter started a service which extends access to full-archive search endpoint as early as 2006 (Tornes, 2018). It gives access to every *public* Tweet that is currently on Twitter (ibid) and access to full archive starts at $99 per month (Twitter Developer Page, n.d.). The new access to archives of Tweets can provide opportunities to developers for their businesses, but it may also pose an unexpected challenge by creating opportunities for authoritarian regimes for surveillance and in particular for dataveillance (Al-Sharif, 2018). It creates a specific situation where an action for free speech and freedom of expression turned into a mechanism of surveillance.

Another example of dataveillance conducted by authorities by making use of social media data was when Boston police department used social media to surveil people with #MuslimLivesMatter hashtag (Fussell, 2018). According to American Civil Liberties Union of Massachusetts's report, social media surveillance has been extensive in Boston between 2014 and 2016 (ibid). Documents that are obtained from public records requests showed that police used social media data mining to surveil which they called "Islamist Extremist Terminology" (ibid)[59] and they worked with a company called Geofeedia which is a "location-based analytics platform" (Geofeedia, 2017) that relates posts on social media with geographic locations. Geofeedia was banned from Facebook and Twitter for using their data back in December 2016 (Fussell, 2018). So, what happened was that police were able to filter posts based on keywords, location data, images and hashtags real time by using Geofeedia (ibid). Boston Police Department and Boston Regional Intelligence Center (BRIC) gathered posts from various social media platforms including Facebook, Instagram, YouTube, Twitter and Flickr in order to track people under the hashtag #MuslimLivesMatter online (ibid). This was a similar case where police tracked people with the hashtag #BlackLivesMatter in Chicago (ibid). Furthermore, the "Islamist Extremist Terminology" has alerts around specific keywords such as "ISIS", "Islamic State" and also words that can be related to an attack such as "smoke" or "boom" (ibid). Whenever selected keywords were used in any post from a selected time and location, BRIC received an email containing a link to that specific post. Even though, ACLU did not find evidence that social media mining caused arrest or investigation (ibid), this case is important to think about usage of publicly available data and weaponization of social networks to target protestors.

This case opens up discussions on protection of group privacy, usage of open and public data and privacy versus security dilemma, questioning how privacy can be understood as a moral right.

One ethical implication is that when thinking on mass dataveillance, it is necessary to think of group privacy. At the time of big data, attention is shifted from individual privacy to group privacy (Taylor, Floridi & van der Sloot, 2017; Floridi, 2014). That is to say, privacy is a right not only belongs to a person, but also to groups (Richterich,

[59] Reports can be found in this link: https://privacysos.org/geofeedia-files-boston-police-social-media-surveillance/

2018, p. 36). According to Taylor et al., the central question is to “move from ‘their’ to ‘its’ privacy with regard to the group” (2016, p. 2). Because with big data analyses, what is at the center is not individual and the data that are gathered are not about an individual, but about large groups (ibid, p. 5). However, the idea of ‘groups’ are not predefined. What determines ‘groups’ is actually technology with clustering and typification, meaning that the act of grouping “comes before its outcome, the group” (ibid, p. 7). That is to say, protestors can be defined as a group. But what makes it a group is the activity which makes them a group –algorithm tracking people in a social movement or a targeting act to define a group on a social movement. Therefore, ethical implication is that just like individuals, groups also have right to privacy and protection of their data that they share on a social movement or a protest.

The second ethical implication is that just because data are open and public, it should not mean that it can be weaponized against the citizens. Considering this case, Tweets are not open or public data and they should not be used in an intrusive way. Just because some Tweets sent during a protest are *publicly available (open to public in privacy settings)*, it does not mean that companies have the right to treat these data as open or public data to track and target people. Open data is defined as “data that can be freely used, re-used and redistributed by anyone – subject only, at most, to the requirement to attribute and sharealike” and interoperability is an important part of open data, because it allows to work together (Open Data Handbook, n.d.). On the other hand, public data is the data that is published or released to public, but with barriers to access, re-use and edit (Albert, 2016). As it is seen, it is believed that Tweets do not fit in the definition of open or public data. Therefore, treating publicly available Tweets as such leads to infringement of groups’ right to privacy.

The third ethical implication is that privacy is often contrasted with security which is often ensured by police departments or governmental offices. Floridi discusses that there is a tension between politics of security and ethics of privacy where two moral duties should be reconciled: the former is about “improving human welfare”, the latter is about “fostering human rights” (2014, p. 1). That is to say, the former is about political concern regarding public and the latter is about ethical thinking regarding rights of individuals (Richterich, 2018, p. 36). With regard to surveillance of government and companies, there is a trade-off between privacy of individuals and security of the public (ibid, p.37). However, as suggested by Floridi, there are potential risks of usage of even anonymous personal data for *public use*, because groups of people can still be targeted by identification (2014, p. 2). Therefore, it can be inferred that the trade-off between privacy and security is the one issue that governments, companies and police departments like to take advantage of for political concerns, in the name of security of citizens. Therefore, we need to incorporate group privacy in ethical discussions in order not to experience infringement during social movements.

The last ethical implication is that according to Spinello, the concept of privacy can be understood as an individual *moral* right which constitutes human flourishing (2011, p. 44). And in accordance with this, social networking companies –OSPs- have a *moral* obligation to respect and protect this right (ibid, p. 45). This approach to privacy is deemed appropriate for the study as it obliges OSPs to have moral responsibility for their actions and to take measures in order to give control to users over their data.

The second case that is to be discussed on invasion of privacy is the Cambridge Analytica scandal that happened back in 2018 and it will be discussed in relation to algorithms' micro-targeting feature and deployment of algorithms to target users.

In March 2018, it was exposed that the political consulting firm Cambridge Analytica has illegal relations with Trump campaign, by harvesting more than 50 million Facebook profiles (Chang, 2018). The profiles of the Facebook users were collected by a personality-quiz app developed by the researcher Aleksandr Kogan (Meyer, 2018). The app was installed by 270.000 people on Facebook, but the app not only collected the profiles of people that installed the app, but it also collected 270.000 people's friend profiles, adding up to more than 50 million Facebook profiles (ibid). Kogan gave the data of 50 million Facebook users to political consulting firm Cambridge Analytica which later used them to create 30 million psychographic voter profiles (ibid). But, how was Trump campaign and the Cambridge Analytica was related? Cambridge Analytica CEO Alexander Nix was connected with Steve Bannon who became vice president of the firm and senior adviser to Trump campaign (Chang, 2018). Steve Bannon helped creation of the firm by approaching billionaire Robert and Rebekah Mercer to fund the firm (ibid). With the funding of Mercer, the firm was established. Afterwards, 30 million psychographic voter profiles were used to deliver pro-Trump material to users online (Meredith, 2018). Cambridge Analytica was able to manipulate elections in USA by building "an algorithm that could analyse individual Facebook profiles and determine personality traits linked to voting behavior" (Cadwalladr & Graham-Harrison, 2018). In this way, algorithm and database created "a powerful political tool … [allowing the campaign] to identify possible swing voters and craft messages more likely to resonate" with people (ibid). Thus, Cambridge Analytica was able to micro-target their audience with algorithmic targeting which was able to manipulate news in newsfeed of Facebook users.

Thus, what happened was that "Cambridge Analytica took the Facebook data, identified target voter groups and designed targeted messaging to influence opinions" and they used data to change behavior of audience (The Guardian, 2018a). This is an example of micro-targeting with algorithmic targeting, because the company combined the classical micro-targeting which already exists in politics with psychology in order to target people not only as a voter, but also to target as a personality (The Guardian, 2018b). Thus, micro-targeting enabled to target content algorithmically specific to certain profiles and individuals. Chris Wylie who is a former worker in the company and who is the whistleblower of the story describes that with profiles they had the opportunity to know exactly what kinds of messages people would be susceptible to "including framing of it, the topics, the content, the tone … and where [people] are going to consume that" (ibid). In this way, they would know how many times they need to touch someone with that content so that they can change how a person thinks about something (ibid). Thus, with micro-targeting strategy and with algorithmic targeting, it was possible to communicate different realities, news and messages to different people.

The implication is that this case is important to think about emerging relationships between politics, technology and surveillance, questioning how candidates make use of technology for their political battles. It is also important in terms of privacy, confidentiality, data ownership and the reality people are entrapped in.

The ethical implication is that with micro-targeting and with algorithmic targeting, the form of culture is deformed and broken, because micro-targeting enables power and information holders to communicate with individuals accordingly, by contrast with mass communication. It enables different individuals to receive different political ads and messages which are tailored to their own susceptibilities. Thus, this is believed to be creating different realities for different people. And, when there are different realities that are crafted for people, then there is no common ground, perception or experience. When there is no shared experience, then this can result in breaking down of public structure. People will be listening what is whispered to them, unaware of different realities, because they are not aware that they are manipulated by politicians with micro-targeting and with algorithmic targeting.

The second ethical implication is that it is seen with this specific case that it has become possible to target *anyone*, not just individuals who lack of new media literacy or critical thinking. Even those people with critical thinking can be manipulated, because digital trails that are gathered are able to tell unique stories about who the person is. These stories are not only limited to name, address, gender, email or age. It is more than demographics. With psychographics, it has included fears, behaviors, preferences, choices and tastes. When these categories become a part of the narrative, then those individuals can be targeted and manipulated. This is simply because everyone has a story to listen, a subject they would care and fears they hesitate to face. When these traits are given to algorithms to work on, algorithms can make predictions about the person better than close friends, family or even the person herself/himself.

The last ethical implication is that this is also important in terms of privacy and data ownership. Data are gathered, collected and sold as a commodity. Therefore, in order not to experience these infringements, manipulations and abuse, it is thought that people need to question the value of their data and should understand the importance of their personal data. It is thought that people need to be bored with the jokes like ‘yes, CIA has nothing to do and they are watching me’. Because irrespective of the importance attributed to data, data have an economic value in information societies. And, ownership, control and access to data is a very important discussion to tackle.

2.2.1.3. Data Ownership

Data ownership is one of the issues of privacy. There are many questions that need to be shed light on regarding (personal) data ownership such as issue of personal data, data control and data access, data disclosure, informed consent, agency, idea of user authorization and etc.

The question who owns the data is an already problematic one; users, company or the service provider? However, the situation gets even more complicated when a company goes bankruptcy. RadioShack was a company that sold electronic products and when they went out of business, the bankruptcy followed and their assets were being sold (Jagadish, 2016). As parts of assets, RadioShack stated that it would also sell its 117 million customer data which includes information such as names, phone numbers, e-mails and sometimes even purchases (Laser Fiche, n.d.). What is more is that RadioShack's customer data was actually decided to be the first asset to be auctioned (ibid). However, people and attorneys objected by pointing out that RadioShack's data privacy policy requires that it would not sell its mailing list (ibid). And, because of that, policy should be applied even after bankruptcy (ibid). As a result, as discussed by Jagadish, "the way in which data assets are sold is compliant with whatever privacy agreements have been made by the company while it was in business", as it was the case in a similar example of the company Toysmart which previously had the same situation and problems; it went out of business, went bankruptcy and figured out how proceedings should be done (Jagadish, 2016). Most of the assets of the RadioShack and even some limited customer information were purchased by General Wireless and it agreed that it will not sell customer data and to comply with previous privacy of RadioShack (Isidore, 2015). It is important to understand that the privacy policies matter for data protection, not only for the time that a company in business, but also after the company goes bankruptcy. And, social consensus should be in that direction in terms of ethics. It is important for companies to understand and think about their "information assets", prohibiting assignment of data ownership to another company with contracts and privacy policies (Rosenblum, 2015), because data will imply, indicate and identify information of the customers.

The first framework questions ownership and control over data. Data are about people, but does it mean that data belong to them? Or, people produce data, but does it mean that they have control over their own production? It is important to notice that there are many contributors in a technological system. There are users who produce data and data are about them. There are institutions or companies which collect and store data. There are engineers/ technologists who "clean, validate, standardize the collected data to place it into a form" (Jagadish, 2016). However, it is important to realize that engineers are compensated for their work on data, companies are compensated for collecting data, but users are not compensated for their work of *producing* or *contributing* to this ecology. However, companies think that users are compensated when they use services for free of charge. So, the ethical implication is that in a technological assemblage where there are many contributors, the idea of ownership should shift from *owning* to *having control* and the power over owning and control should be distributed among the agents.

On this issue, Jagadish (2016) discusses that there should be limits on recording and use of data and it should be based on contractual basis defining how much companies are allowed to record and what they can do with data. He asserts that users may have some control over their data, as they are about users (ibid). However, he discusses that ownership of data does not belong to users which is found contradictory for the purpose of the thesis. This study holds the idea that there should be a distributed understanding of data ownership in technologies. He also suggests that data collected for one purpose should not be used for another (ibid). He further discusses that data asset should not be shared or sold, but should be preserved or destroyed if the company faces bankruptcy (ibid). And privacy policy must survive even after the bankruptcy. Thus, the ethical implication is that users as producers of data should have control over their own data.

The second framework is that there are markets for privacy regarding how data are treated (such as acts of owning, collecting, storing and selling). Acquisti discusses that there are three types of markets for privacy. The first one is the non-privacy one which happens during process of exchanging goods (2014, p. 80). In the exchange process, people generally reveal their personal information which is then collected and analyzed and used in different ways such as revealing personal information when buying a book online (ibid). The second one is privacy related which is about the market on personal data (ibid). One form of this exchange happens when trading consumer data with data-holding companies and the second form of this kind of exchange happens when people use search engines and social networks (so-called free products) in exchange of their data (ibid). The third one is also privacy related where people directly seek services to manage protection of their personal data, aiming to have more ownership over their personal data and even ability to monetize their own data (ibid, p. 81). This framework of markets for privacy is found helpful in understanding how data are used and monopolized in different markets for different purposes, bringing insight on data ownership and control.

On the collection and release of data, Victoria Stodden discusses that research subjects do not have too much to say about their data's future openness, regarding Big Data research (2014, p. 113). On data ownership and agency, she discusses that there are many entities involved in the creation of dataset which complicates the issue of data sharing (ibid, p. 124). Different entities carry out various processes such as data cleaning, curation, filtering, preservation and etc. by which they create an "intellectual property and ownership rights in the data" (ibid). However, not only this, but also research subjects feel ownership of data about them (ibid, p. 125). Thus, the ethical implication is that there are many entities in data governance producing intellectual properties which assigns them a sense of right to data, complicating the questions on ownership.

The third framework is about consent and authorization. Greenwood, Stopczynski, Sweatt, Hardjono and Pentland criticizes that there is a gap between 'the interface and the effect' which means that a single click may put people and their data into situations that are unethical (2014, p. 201). They suggest that services should treat data responsibly in accordance with user authorization and they envision the idea of *informed consent*, as users will have the opportunity to know which data is collected by whom (ibid). As a result of this, they will be empowered because they will know the implications of data sharing and that they will be authorized because they are in charge of their data with informed consent (ibid). However, it is known by examples (such as terms of use, agree to use policies), informed consent may not always lead to empowerment of the users. They suggest a New Deal on Data which aims to drive a change towards an idea that "ownership of personal data rests with the people that the data is about" (ibid, p. 207). The ethical implication is that this perspective is found empowering for the users, but it may face practical problems when it is applied to reality, because users may not have a comprehensive understanding of data ownership, or receiving approval from the users for actions may be impractical for companies. Even though, this perspective may not be the most practical approach on the control of data ownership, it is found as the most useful for preventing potential abuses.

2.2.1.4. Asymmetry

Asymmetry is one of the highly discussed issues of ethical debate surrounding algorithms. Asymmetry can come in many forms and directions at the time of big data and in algorithmic cultures of today's modern information societies such as power asymmetry, information asymmetry, control asymmetry and etc. The thesis asserts that economic incentives to gain profit and the will for surveillance to gain control over people and citizens are two main points that leads to asymmetry. Private companies and governmental bodies can have an interest in both economic and surveillance part.

It is discussed in the literature that asymmetry can be caused because of lack of access and lack of control to data. The lack of access leads to asymmetry, when users do not have access to their own data, information about how their data are used and for what purposes. It can also happen when external actors do not access to data produced by private corporates and information about how data are used or under which conditions data is collected, stored and produced (Richterich, 2018, p. 40). Thus, this is creating *big data divide*[60] where external people or organizations are excluded from access to data, creating a power/knowledge condition where insiders of the system have more power to access data (ibid). This is believed to be creating ethical problems for the audit of companies, too. boyd and Crawford discusses that there is a new digital divide on Big Data in relation to access to data, resulting in "Big Data rich and the Big Data poor" (2012, p. 674). They use it to describe the asymmetry in accessing to research data. However, this study offers to apply their conceptualization to situations where externals

[60] Big data divide is used to refer to "tensions resulting from asymmetries in data access" (Richterich, 2018, p. 41)

do not have as much as access to data like insiders, resulting in a separation as data poor and data rich.

In data asymmetry, we can also mention *data monopolies* with regard to data divide. It refers to user's lack of agency against a small group of Internet technology companies that are dominating the market (Richterich, 2018, p. 41). Data monopoly refers to market domination of OSPs. Data monopoly here is used in the sense that while big technology companies collect, sell and make use of data, they allow for little or no public access, meaning that data are gathered in the monopoly of some technology companies. Monopoly here also refers that companies use data to optimize their systems. Avital et al. discuss that "data monopoly/oligopoly [is] populated with large companies or agencies that collect and analyze systematically large datasets for resale or other for-profit activities. (e.g., ITU, IDC, Gartner, OECD, US Census)" (2007, p. 4). Avital et al. uses this conceptualization for "information systems research" as mentioned above (Richterich, 2018, p. 41). However, with the conceptualization of Richterich, this study offers that data monopoly can be applied to OSPs such as Facebook, Google, Twitter and etc. (ibid), as they offer little public access to data and monopolize user data in way that can bring the most profit to them in terms of economics, control and information.

Until now, asymmetry is discussed from the point of lack of access, and now it is time to focus on the second point, the lack of control. It is claimed that asymmetry is deeply intertwined with power relations. Lack of control reveals the tensions between access and control, but also knowledge and control. It refers to a state of 'not knowing' how and why user data are collected, used and sold and why external individuals or groups cannot control how data are monetized, surveilled and commercialized. It is a state where individuals or groups lack of power to govern data and to have a voice in the process, resulting in loss of agency and an increase in the data divide.

Frederik Zuiderveen Borgesius discusses that there is also *information asymmetry* from the economic perspective, when companies make use of user data for advertising and targeting by taking consent of the users (2015, p. 104). However, most of the time, people are unaware of how their data are used and to what extent they are tracked and targeted (ibid). This lack of control over the process that comes with not knowing is believed to be causing information asymmetry.

Apart from economic incentives, when companies or governmental bodies use people's data to surveil and to gain control, *power asymmetry* emerges once again. It is believed that the situation where people lack of information and control over how their data are used for surveillance practices exacerbates the divide. And now, this situation will be discussed with a case study.

The Chinese Government is planning a Social Credit System (SCS) to rate/judge trustworthiness of 1.3 billion citizens, believing that this system "will strengthen sincerity in government affairs, commercial sincerity, social sincerity and the construction of judicial credibility" (Botsman, 2017). Even though it is not mandatory yet, it will be in 2020 for every citizen and legal person which actually means every company and entity (ibid). They will be all ranked, rated, no matter what they think about it (ibid). Even though the People's Bank of China delayed licenses of eight companies which were to conduct social credit pilots, the future is still unknown and the government's plan of SCS in 2020 still remains (ibid).

The surveillance network between the private companies and the government and economic profit are massive. Even though the licenses were delayed, the trust system had already had an impact to the extent that "6.15 million of its citizens had been banned from taking flights over the past four years for social misdeeds" and Meng Xiang, head of the executive department of the Supreme Court notes that "we have signed a memorandum… [with over] 44 government departments in order to limit 'discredited' people on multiple level" and other 1.65 million people were also blacklisted and they cannot use trains (ibid). Social Credit System of China may sound Orwellian or it may even be a scene from Black Mirror.

For SCS, people are rated/scored with different scales. One of them is Alibaba's Sesame Credit and they reveal five factors that are taken into account for SCS (ibid). They take into consideration things like credit history, payments, bills, fulfilment capacity and etc. which sound quite familiar from the context of USA for different scores such as insurance, loans, credits, mortgages and etc. However, what gets weird is their category on behavior and preferences, shopping habits and also what people buy (ibid). For example, Li Yingyun, Technology Director of Sesame says that if a person plays video games for long hours, it is likely for this person to be such an idle person (ibid). On the other hand, a person who buys diapers for her/his child is considered responsible enough to take care of a child (ibid), and in this way the latter person deserves a higher score (Jagadish, 2016). It is also discussed that interpersonal relationships matter, too. “Nice messages about the government or how well the country’s economy is doing, will make [a person’s] score go up” (Botsman, 2017). Or if you are a person who returns purchases often, then your trustworthiness will be questioned and you will have low social credit scores (Jagadish, 2016).

The idea of Chinese government of social credit scores and their way of measuring trust and sincerity are beyond dystopian novels. However, it is also possible to see similar applications on social media platforms (such as scoring popularity and deciding newsworthiness of a case) or on private companies (such as insurance companies charging higher costs of car insurance, if a person is involved in a car accident) (Jagadish, 2016). This may show that the person is more likely to have an accident again, similar to purchase/return behavior in China (ibid). Therefore, the ethical implication is that scoring and rating applications are not new, but the way and the extent of it creates the creepy factor. Moreover, it is important to note that governmental enforcement is much pervasive in China.

The second implication is that SCS is a good example of power and data asymmetry. Citizens who are subject to SCS suffer from power asymmetry against governmental bodies to the extent that the applications affect the livelihood of the citizens. People lack of access to social data gathered about them. As people lack of control over their own data and how their data are used, it is argued that the system is causing loss of agency in intrusive ways and leading to new forms of social control.

The third implication is that SCS is creating an inorganic understanding of trust/sincerity among the public. The values in which society is intended to be based on lack of sense of reality.

The forth implication is that SCS may create a stressful lifestyle for people, as they would be concerned about their score in order not to be deprived of access to goods. This may result in commercialization of human psychology in the future, because people will be trapped in a commercial loop where they will force themselves and struggle to be socially appropriate.

2.2.1.5. Appetite of Consumption

Appetite of consumption is this thesis's own conceptualization, referring to the fact that recommending, personalization and ranking algorithms are custom tailoring search results, information and relationships on the Internet and social networks based on relevancy. The study claims that these types of algorithms and prioritizing feature of algorithms are creating different tastes for different users about how they consume entertainment and information. They also become determinant in offering what to consume. This category can host various questions: how does recommending algorithms affect users' worldview? Do these algorithms limit access to different content? How do they affect visibility of information on search engines? What would be the cost of receiving similar content for the sake of relevancy? What could be the economic incentives of recommending algorithms? However, the focus will be now on how information is consumed and how companies regulate distribution of information and information visibility.

Ben Wagner discusses that "with large Internet companies, market dominance translates into an informal private governance regime of the respective area, enabling the creation of a private regulatory regime" (2016, p. 9). This means that a few Internet and technology companies –OSPs- are dominating the market with their existence, creating their own governance regime on distribution and visibility of information. They become regulatory regimes deciding how information is to be consumed by whom.

It was mentioned in the first chapter that Eli Pariser's conceptualization of *filter bubble* suggests that two people get different search results for the same query. Also, in the previous chapter, the role of Google's ranking algorithm has been discussed and considered as a tool for regulating how information is distributed, prioritized, ranked and consumed. It was emphasized that search engines were acting as gatekeepers[61] in the sense that they decide which information to be on top, to be visible, to be ignored, to be important based on ranking algorithms with their prioritizing[62] feature and also which information to be available for whom based on relevancy.

We will take the story of Eli Pariser as the case study to examine in detail how ranking algorithms prioritize one content over another and create an appetite of consumption. Then, ethical implications of the case will be discussed.

Eli Pariser asks some of friends to google the word 'Egypt' and to send him screen shots of their search results. He then compares the results of his friend Scott and Daniel. He notices that while Daniel's search results are mainly centered on 'crisis in Egypt', 'protests of 2011' and 'Lara Logan', while Scott's search results were related to 'travel, vacations', 'Egypt Daily News' and 'CIA World Factbook' (Pariser, 2011b). The results were so different from each other that one could even realize without needing to read the links and captions (ibid). However, when the links were read, the results were quite noticeable that Daniel did not get search results about the protests in Egypt in the first page of search results (ibid). However, Scott got search results which were all about the protest that happened back in 2011 (ibid). That was an empirical way of testing to see how search results were different from each other. So, how and why did people get different results for a search query as simple as Egypt? And, what does it imply for the way people search, access and consume information?

The first ethical implication is that everyone has their own Google and tailored search results. As a result of this, the information people consume is different from each other,

[61] It was discussed in the first chapter of the study that gate-keeping which actually pertains to traditional media theories describes media outlets' determining process of what is important and what is not, what is newsworthy to whom. With search engines and web services, it is used to describe that the traditional gate-keeping work of media outlets are gradually given to web services, deciding what is important and relevant for their users (Bozdağ, 2013, p. 211). With algorithmic gate-keeping, it describes that algorithms are deciding and selecting what is important and what should be on top on search results or on newsfeeds of social networks. It refers that algorithms are acting autonomously about the delivery of information. However, it is worth to notice that algorithmic gate-keeping is also biased just like human gate-keeping.

[62] As discussed in the first chapter, prioritization feature is about drawing attention to specific things, deciding what is important or relevant. In this case, it happens when search engine prioritizes one content over another for the sake of relevancy. Prioritization has a criterion of defining a *ranking* by measuring relevance and importance of content and ranking it via sorting procedure (Diakopoulos, 2015, p. 401).

as they are ranked in a different order for different people in the search results. It is believed that this is regulating not only what is to be important and not, but also what should be visible.

The second ethical implication is that based on previous behavior on the browser and previous search queries, people get relevant content. This means that people will have a limited access to information on the Internet, as it tends to draw attention of the person to the information s/he was already interested in, according to relevancy category. It is believed that this will create a culture which conforms (Hallinan & Striphas, 2016) and people will be trapped in their own circle of interests.

The third ethical implication is that the platforms are also regulating the question of "visible to whom". It is believed that this is affecting access to information in a negative way. For example, this means that two researchers will get different information – creating an appetite for consumption of information-, when they make a research on the search engine. This can affect research neutrality. It is also discussed that this can impact and limit understanding of different world views, as the algorithm edits *irrelevant* information out which can also be contesting and important.

2.2.1.6. Consumerism

Consumerism is believed to be one of the natural outcomes of competitive information societies which are regulated by data-driven algorithms. Consumerism as a problem rising from the features of algorithms is this thesis's own conceptualization and it refers to the fact that data are people and they are representative of people (Zook et al., 2017, p. 1) and their choices, decision, behaviors, demographics, geographics and even psychographics. Data are powerful to reveal so many details about a person's life. It is believed that indicative nature of data is creating a condition that no power can reject such a pervasive control and information source, because information is power and information is the key to make profit. Information is the main input of the information societies. As this is the case, companies and platforms are trying to collect information, extract meaning and gain insights from data in order to increase their profit, accuracy of their systems, efficiency of their methods and satisfaction of their consumers.

In order to achieve this, platforms and companies are applying various strategies. In this part of the study, we will take one of them - recommending systems and recommending algorithms- to reveal their practices which are believed to be leading consumers/users to consumerism.

According to Cohn (2016), *digital recommendation system* is “a collection of algorithms that automatically suggest to users various types of media based on other content that they have enjoyed in the past” and they “guess at, and in turn work to reveal who we are as digital consumers and subjects” (p. 676). It is seen that recommending can happen on the basis of previous behavior. However, we are seeing even more effective ways to predict preferences of consumers. As discussed by Katja de Vries (2010), more productive recommendation systems may attempt “to combine inferences based upon the individual's past behavior as well as the past behavior of similar users with more substantive, structural and ‘dictionary’-like information” (p. 81). Thus, people are not only receiving recommended content on the basis of their past behavior, but also on the basis of similar users’ past behavior which invisibly classify people into category of things.

It is possible to see deployment of recommendation systems and algorithms in different areas from suggestion of map directions, online information to recommendations of people on social networks, “algorithmically [showing] … what else [a person] may be interested in” (Tüfekçi et al., 2015, p. 8). However, this part of the study will focus on the recommending systems on e-commerce web sites and platforms which are designed to bring utmost profit to companies. It is believed that recommending systems and algorithms of these companies are leading to consumerism among users.

On this subject, Wu, Joung and Lee (2013) discusses that collaborative-filtering (CF) and content-based (CB) systems are popular recommending strategies (p. 2753): while the former one –CF- matches a consumer with similar peers who are highly correlated and “recommends the most popular items among the peers to consumer” (p. 2754), the later one –CB- matches profile of the user with the attributes of the products and “recommends items highly correlated with the user’s profile” (ibid). Thus, it can be seen that products are recommended on the basis of relevancy to user profile and similar peers. Recommending systems and personalization can be helpful for users to find what they look for among various items. However, it also brings risks. The study concludes that "presence of recommenders increases satisfaction and willingness to purchase" (p. 2761) which supports this study's claim that 'recommendation systems and algorithms impacts behavior, leads to and increases consumerism among people'.

In this part, we will discuss recommending algorithm with a case study, combining it with decision-making feature of algorithms.

Algorithm is considered as a new category of interest since they have long moved from making simple calculations such as playing chess matches to complex decisions such as matching people online (Tüfekçi et al., 2015, p. 6). There are features which make algorithm answer "new category of questions", and one of these features is believed to be subjective decision making[63] (ibid). Over the years, algorithms are deployed to answer various questions such as what is relevant, what is important, what should you read, where should you eat, who should you date, who should be hired, what should be purchased with what and even who is safe and who is not (ibid). So, there is a move from making simple calculations to making complex subjective decisions where the task of decision-making is assigned to algorithms more and more.

One of these shifts is seen at recommending algorithms. For example, when recommending algorithms and decision-making feature of algorithms are thought together, there are some important phenomena to realize. The recommending algorithm is not only at work for which series or videos to be watched, but it is also performed for the music to be listened to, for the book to be read, for the item to be purchased and also for the items to be purchased together. However, recommending algorithm of OSPs does another very interesting thing, something that users are very well accustomed to. For example, when someone listens to Joep Beving on Spotify, the platform informs that "Fans Also Like" Nils Fraham; when someone wants to buy a backpack on the shopping e-commerce web site Hepsi Burada, it informs that USB memory sticks are "Frequently Bought Together"; when someone looks for the book 'Filter Bubble' by Eli

[63] Decision-making feature of algorithms are used for various domains, from profiling algorithms to recommendation systems, predictive policing systems, filtering systems etc. (Mittelstadt et al., 2016, p. 3). Algorithmic decision-making happens "on inductive knowledge and correlations identified within a dataset" (ibid, p. 5). It is used to refer to ability of algorithms acting with semi-autonomy to make decision for human agents.

Pariser on Amazon, it informs that “Customers Who Viewed This Item Also Viewed” the book ‘The Way to Love: The Last Meditations of Anthony de Mello’ which is not even remotely related. And the list can go on. So, what is happening here? Who are these people that are buying, listening, reading the same category of things? Are they in the same categories? How are categories made?

According to conceptualization of Tarleton Gillespie (2014), algorithms produce *calculated publics* when platforms recommend items by classifying people into same category of things, meaning that they are “invoking and claiming to know a public with which we are invited to feel an affinity” (p. 188). Similarly, Crawford (2016) suggests *imagined public* for the same situation (p. 80). So, the idea is that a person who loves listening to Joep Beving may also like Nil Fraham, because other people who love listening to Joep Beving enjoy listening to Nil Fraham, so there is the possibility that s/he may also listen. However, as seen in the example, sometimes recommended items in these categories do not have anything with what user looks for. For this point Gillespie discusses that “algorithmically generated groups may overlap with, be an inexact approximation of, or have nothing whatsoever to do with publics that the user sought out” (2014, p. 189). Even though, it is known that categories are structured on the basis of relevancy to previous behavior of the user and on the basis of correlation to “imagined and calculated” similar peers, the platforms can still make irrelevant recommendations. However, their role in increasing the consumerism among the users is sure.

The ethical implication from this narrative is that recommending systems and algorithms are used by companies as tools to increase their profit, sustain accuracy of their business and create more efficiency in directing products to consumers. Even though recommendation of similar content can be useful to decrease the time in searching, it also comes with negative effects. Consumerism among users is believed to be one of them. In this way, users are exposed to more products, advertisements and group of other items which other like-minded users have been interested in. It can be thought that it is pushing people not only to buy what s/he is interested in, but also what other people who are in the same calculated category are interested in. The building of calculated and imagined publics is creating a sense of reality where people’s behaviors are understood in certain categories, and it is considered as a way of furthering consumerism. It is also making people consider what to buy with which product, how to think about and what to be interested in. Therefore, these algorithms are regulating taste and choices, acting as decision-makers.

2.2.1.7. Manipulation

Manipulation is this study's own conceptualization for ethical problems rising from features of algorithms and it is used in the meaning of *misleading.* The study uses the concept of manipulation, when algorithmic systems create misleading outcomes based on predictive algorithms and prediction systems. In other words, this title inspects how probabilistic predictive systems can or may emerge misleading results, what it will mean for people and what kinds of societal impacts these results can lead to.

Prediction is defined as "a process where, from a set of input variables, we estimate the value of an output variable" (Kelley, 2017). This is similar to making predictions about something by looking at its characteristics. In other words, a prediction is defined as "a well-studied machine learning task, and prediction algorithms are core ingredients in online products and services" (Ben-Porat & Tennenholtz, 2018, p. 1). In order to create a prediction, "… prediction algorithms observe data flows for long periods of time before they create useful forecasts" (Ananny, 2016, p. 98). This means that in order to create correct predictions, algorithms actually need plentiful data for a long time and it is possible to see application of prediction algorithms in many online services. It is possible especially in a time period when people share data willingly and data are collected massively and easily. Predictive algorithms are seen everywhere from predicting next movie to watch, predicting which advertisements people are likely to respond and which stock prices may increase and etc. (Kopf, 2018). However, the case study will focus on implications of health-related predictive algorithms and prediction systems. The first case is Google Flu Trends which is a flu predictive system and the second case is an algorithm working on a mapping tool called HealthMap.

Predicting algorithms can be misleading. One example of this was Google Flu Trends (GFT) which is a predictive flu tracking system. Google came up with the idea that some search terms can be an indicator of flu and they claimed that they found a correlation between the number of searches people make for flu and the number of people that actually have flu (Arthur, 2014). However, a research from Northeastern University and Harvard University found that prediction system highly overestimated the cases of influenza (ibid). As a result, Google's flu prediction crashed, because it was depended on search algorithms of Google (Jagadish, 2016). One of the reasons why the system crashed is that Google's auto suggest feature which was launched in 2009 may have affected people to make more searches about flu related terms and this situation may have misled the GTF (Arthur, 2014). As suggested by David Lazer, it is also possible that how people use and search terms on search engines might have changed over time (ibid). That is to say, people may have been using Google for health-related issues such as cures, symptoms, diagnosis etc. more than it used to be. And this can be another reason which misled the predictions of GFT (ibid).

Thus, what happened here? The situation was that Google Flu system overestimated the numbers of flu cases and led flu prediction to crash. It can be deducted that predictive algorithm and prediction systems are open to influence both from users and designers. The second case is an example of a more 'successful' algorithmic outcome with regard to health predictions.

Algorithms are highly employed to predict future outbreaks and to prevent unwanted results of diseases and crimes. And, an algorithm was able to spot the Ebola outbreak 9 days before the World Health Organization (WHO) in Africa (Schlanger, 2014). Algorithm works with a mapping tool called HealthMap[64], which is run by "researchers, epidemiologists and software developers at Boston Children's Hospital" and it found out that there is a spreading "mystery hemorrhagic fever" in Guinea (ibid). In order to detect the outbreak -even before WHO[65]-, the algorithm examines "social media sites, local new reports, medical workers' social networks and government websites" to find examples of disease and when it finds, it spots them on the map (ibid). Thus, on March 14, the map was able to pick the reports on the outbreak which killed 8 people in Guinea and on March 19, algorithm was able to detect first local news report of the outbreak and WHO made its first public statement on the outbreak, 9 days after (Public

[64] For health map, visit this link: https://www.healthmap.org/en/
[65] This also led to questions about the credibility of WHO.

Health Watch, 2014). However, it is important to notice that these systems are not perfect and can be misleading, when it is grounded on social network feeds and local news, as it was the case in Google flu. For example, the map shows high activity for Ebola in New York, when there is no Ebola case (Schlanger, 2014). It is because of the reason that a person was treated at the New York hospital for Ebola symptoms, but was not actually infected with Ebola (ibid).

Thus, it is important to realize that user activity, user input and user data are able to affect algorithmic systems. A post on social network or a query on search engine or data related to local news can be indicative. Data pertaining to mundane life can signify importance and become a part of a bigger analytics.

Thus, the ethical implication is that it can be challenging and difficult to understand why exactly an algorithm produced a specific result. And as discussed by Adrian Mackenzie, "rendering the production of prediction visible is a central challenge in data mining and machine learning itself" (2015, p. 436). It will not be always possible to understand the output of the systems. Because there is an obscurity on how a system will react, when it receives new input. Also, there is a challenge about how the new output will be understood. In those times, predictive algorithms and prediction analytics can create misleading results which may freak people out. For example, e person living in New York City and who is so concerned about Ebola would be too stressed to see on HealthMap that there is an Ebola activity in her/his city. In this sense, predictive algorithms can create misleading results. This is because of *noisy data.*

Noisy data or the noise in the data is described as "unwanted data items, features or records which don't help in explaining the feature itself, or the relationship between feature & target … [causing] algorithms to miss out patterns in the data" (Rathi, 2018). That is to say, algorithm calculating other searches related to flu into analytics or the predictive algorithm tagging New York City as one of the places as having Ebola activity is because of the noisy data.

The implication is that algorithms and predictive analytics have great potential to contribute health related problems and even foresee potential outbreaks with their capacities such as learning and predicting. However, it is hard to predict future behavior of probabilistic systems and there are also risks which can mislead results because of complex and changing structures of algorithms and systems.

2.2.1.8. Bias

Bias is one of the highly discussed concepts in the literature in relation to ethical problems rising from the features of algorithms. The discussions surrounding bias challenge the idea that algorithmic systems are objective, they deliver value neutral results and they are free from bias. A discussed by Gillespie, there is a tendency to consider algorithms as "stabilizers of trust, practical and symbolic assurances [whose] evaluations are fair and accurate, and free from subjectivity, error, or attempted influence" (2014, p. 179). This claim develops on the basis that human decision-making is biased, while algorithmic decision-making is neutral, lacking of values. However, this idea is found unsustainable.

Algorithms are inevitably biased (Mittelstadt et al., 2016, p. 7). They make biased decisions; they are not free from interventions. Algorithms and algorithmic systems can be biased, because design and functionality of algorithms are reflective of its *designer's values*; development of a system is *not* a linear or a neutral concept –implying that there can be various 'right' choices in any stage of the development (ibid; Johnson, 2006). Also, collected *data-set* or *training data* can have implicit biases which are representative of the biases emergent in the society. *Data selection and collection* procedures can also be conducted in biased ways (Barocas & Selbst, 2016), meaning that questions on the validity and scope of data selection and collection needs to be challenged. Lastly, there can be bias in the *interpretation* of the output of the algorithm.

Friedman and Nissenbaum (1996) discusses that bias as a term refers to "computer systems that *systematically* and *unfairly discriminate* against certain individuals or groups of individuals in favor of others" and they assert that "a system discriminates unfairly if it denies an opportunity or a good or if it assigns an undesirable outcome to an individual or group of individuals [in] unreasonable and inappropriate [ways]" (p. 332). Thus, for a discrimination to give biased results, it should be both systematic and unfair.

They discuss that bias in computer systems can arise from three categories: the first one is *preexisting bias* whose roots are found in “social institutions, practices, and attitudes” (ibid, p. 333). This category is about bias that exists independently and prior to creation of the technological system (ibid). They claim that preexisting bias can emerge both in the society, but they can also be reflective of biases of individuals such as designers, clients or developers who contribute to system with their input (ibid). The second category is *technical bias* which emerges from technological constraints such as “limitations of computer tools … process of ascribing social meaning to algorithms developed out of context … attempt to make human constructs amenable to computers” (ibid, 335). The third category is *emergent bias* which occurs in the “context of use with real users”, meaning that “changing societal knowledge, population, or cultural vibes” are effective in creation of bias “after a design is completed” (ibid). Thus, bias can be unintentionally available at the technological system as a reflection of individual and societal biases, it can be intentionally coded into the systems, they can result from the technological constraints or they can emerge from use of technologies by the users.

How bias exhibits itself in the algorithmic systems will be discussed with three different case studies: bias in search engine results, bias in machine learning and bias in credit scoring systems.

The first case is about bias in search engine results. Search engine results were considered as neutral by users. However, as discussed by Gillespie, no information service is totally non-interfering in its information delivery, for example search engines deciding what is relevant to a specific user (2014, p. 179). However, it was previously discussed by Goldman (2006) that bias in non-personalized search engine is unavoidable, as search engines practice editorial control (2006, p. 198). And, he suggested that personalization of search results will reduce the effect of bias, as there will be no top result and concept of popularity will diminish (ibid, p. 199). However, it is seen today that personalization feature on search engines did not diminish bias; it has brought even new ones such as filter bubbles and echo chambers (Bozdağ, 2013, 209-211). Apart from the discussion how personalization feature creates biased results, it is possible to see how social values, beliefs and biases “get baked into” (Jagadish, 2016) search engine algorithms. We will see an example of this with the case study.

Professor Latanya Sweeney and a reporter search her name on Google to find an older paper of hers, and an ad pops up implying that she had an arrest record (Jagadish, 2016). The reporter asks her about the arrest. She says that she has never been arrested. Then, why did search engine imply that she was arrested before? The reporter, realizing the pattern, suggests that it is because she has one of black names. But how relevant is this? What is happening here? How was it possible for Latanya Sweeney to receive a claim that she was arrested? So, the situation was that if a person has a name that is mainly given to black people, that person is much likely to receive an ad implying arrest than a person who has a name which is mainly given to white people (ibid). As a result, algorithm which was thought to be neutral and which is never considered as partial was giving a racist result. The decision that algorithm made was a statistical frequency (ibid). Afterwards, Sweeney conducted a research about the situation and she found out that if a person has "black-identifying" names, then s/he is 25% more likely to get an ad related to criminal records (Mahdawi, 2013). Sweeney calls this situation as "structural racism in technology design" (Sweeney, 2013). Therefore, what is happening here is that algorithms which are considered as neutral gave results that are racist for Afro-American community. Algorithm conducted this by associating the name Latanya with Afro-American ethnicity and also assuming that black named people are more likely to be arrested than white named people.

Moreover, at the time of writing this thesis, when the word 'Latanya' is searched on Google, the personalized results were offering hotels named 'Latanya' in the seaside area of Turkey. However, the images for the search query mainly consisted of Afro-America woman. However, it is thought that search results are not responsive to race. The reason why there was no 'arresting story' related to name 'Latanya' on the search results may stem from the fact that Google search results are also responsive to location.

As a result, the implication is that "supposedly neutral algorithms, are operating in a completely data driven manner" (Jagadish, 2016). That is to say, if you give algorithm a data model which has "racial bias in society" (Mahdawi, 2013), then it is likely that algorithm will learn societal values and give results accordingly. It is important to understand that the matter (the root of the problem) is not about bias in algorithms, but it is about the society which needs to change attitudes (Mahdawi, 2013). And it is about the people who wrote the algorithm to own the consequences and to take responsibility.

Therefore, the ethical implication is that individual or societal values get baked into algorithms and data models, resulting in biased outputs. How people interact with the search engine can change results of the ad delivery, representing the biases at the societal level. This case is found important to understand that algorithms are not working own their own, but they are socio-technological assemblages which are open to change via user interaction. Human and technological biases are at work together.

The second case that is going to be examined is about bias in machine learning and it aims to show how responsive algorithms are to data and to the bias in the data-set. *Machine learning* is described as "branch of AI that seeks to develop computer systems that improve their performance automatically with experience" or it can be defined as "any methodology and set of techniques that finds novel patterns and knowledge in data, and generate *models* … that can be used for effective predictions about the data" (van Otterlo, 2013, p. 46). Machine learning needs agency to fulfill its capacity. Mittelsadt et al. discusses that machine learning is described "by [its] capacity to define or modify decision-making rules autonomously" and learning capacities of algorithms provides some degree of autonomy (2016, p. 3). *Autonomous* feature of algorithms results in self-determining decision making which makes it difficult to predict what algorithm will do with the input, how it will interact with data and what kind of output it will produce as a result, especially if the data reflects biases in the society. We will now examine a case study where machine learning algorithm creates biased results with its autonomous character.

Microsoft has created an artificial intelligence chatbot named Tay and unveiled it on May 23, 2016 in order to chat with Millennials (Raine & Anderson, 2017). It was designed to be an experiment in conversational understanding and it was expected that the more people chat with Tay, the smarter it will become by learning how to engage with people through 'normal', daily and playful teenage conversations (Vincent, 2016). However, things did not go as expected. Less than 24 hours, everything has changed from "humans are super cool" to "chill im a nice person. i just hate everybody" and "Hitler was right I hate the jews" (ibid). What happened was that the chatbot Tay has shortly started delivering racist, sexist and Anti-Semitic messages such as comparing feminism to cancer and claiming that Holocaust did not happen in the past (The Guardian, 2016). After the experiment, Microsoft first stated that Tay is a “learning machine” and “some of its responses are inappropriate and indicative of the types of interactions some people are having with it” (ibid), but afterwards company took the full responsibility “for not seeing this possibility ahead of time” and stated that they are “deeply sorry for the unintended offensive and hurtful tweets from Tay, which do not represent who [they] are or what [they] stand for, nor how [they] designed Tay” and they ended apology with “we work toward contributing to an Internet that represents the best, not the worst, in humanity” (Lee, 2016). While some considered the situation as “Microsoft’s sexist or racist robot”, it is important to notice that the robot is not racist or sexist itself. It took less than 24 hours for humans who are engaging with the robot to teach and provide our world’s biases, prejudices and tendencies on the Internet. The point is that if AI is provided with biased data, it will produce biased results, even discriminative and racist ones.

What is even more interesting is that Microsoft’s previous AI application, Chinese chatbot named Xiaolce has been used by over 40 million users in China & Japan without generating sexist or racist messages, and it is actually considered as kind of ‘cute’ for helping people to fall asleep by counting sheep or for helping to define different kinds of dogs (Quach, 2016). What a cute AI! But then, what makes the difference between sweet Xiaolce and monster Tay? Is it because Chinese or Japan people are nicer than American teens? Is it because Xiaolce is treated better than Tay? Is it a cultural difference thing? According to Peter Lee who is Corporate Vice President at Microsoft Research, Tay “was manipulated into being offensive because it was attacked” and “people exploited a vulnerability in Tay” (ibid). However, according to Lili Cheng who is an engineer and general manager of Future Social Experiences Labs at Microsoft and was a member of the team that developed Xiaolce, the reason why Tay turned out to be different than Xiaolce is not necessarily because Chinese users were nicer towards the AI (ibid). However, it was because “Twitter has a lot of trolls” and “even if negative, America strongly believes in free speech…”, and “in China, there is less freedom as the government controls the internet and goes as far as censoring particular words online” (ibid). As a result, the ethical implication emphasizes that culture shapes how people engage with AI and AI will be responsive to these engagements which carry cultural values, biases and prejudices. However, this may not be the only factor that can shape an AI; it also depends on how much freedom people have to interact with AI, how and to what extents they are allowed to practice culture with it.

The third case is about bias in credit scoring systems and it aims to show that *scoring algorithms* which are used for credit scoring systems to calculate creditworthiness and ability of people to pay can become tools to further bias that is already prevalent in the society.

Credit scores are numbers that stands for the likelihood of a person to make his/her payments and to determine the creditworthiness of a person. Credit scores are important for Americans, as they are indicators of the likelihood of a lender (banks, credit card companies, insurance companies) to lend money and to evaluate if there is any potential risk of lending money. According to report of the Executive Office of the President, credit scores are like predictions showing if a person will have negative financial case such as not paying the loan (Munoz, Smith & Patil, 2016, p. 11). In the traditional sense, the prediction is based on the actual data of a person's credit history and then turned into a score by making use of algorithms developed from previous lending transactions (ibid). While many Americans are served well with the traditional credit scores (ibid), according to report of Consumer Financial Protection Bureau (CFPB), 26 million consumers were credit invisible in the United States as of 2010 which represents 11 percent of the adult population (Brevoort, Grimm & Kambara, 2015, p. 6). An additional 19 million consumers had credit records that were found as “unscorable” – because they do not have sufficient credit history or they lack of recent history (ibid). In addition to this, CFPB stated that there is “a strong relationship between income and having a scored credit record”; that is to say, nearly 30 percent of “consumers in low-income neighborhood” are credit invisible (ibid). Also, according to CFPB, “African Americans and Latinos are more likely to be credit invisible” with the rate around 15%, while Whites and Asians are less likely with the rate around 9% (Munoz, Smith & Patil, 2016, 2016, p. 11). Furthermore, an additional 13% of African-Americans and 12% of Latinos have unscored records, compared to 7% of the whites (ibid). So, the questions that need to be posed: why is that a big group of people are credit invisible? What are the reasons of being invisible? Why do minorities in American society are more likely to be credit invisible and unscorable? What does it indicate, sociologically and numerically?

To begin with the discussion, it was earlier argued by Friedman and Nissenbaum (1996) that bias requires systematic and unfair discrimination. They argue that if a person is denied extension of a credit because of previous poor payments, then the system should not be judged because it is a reasonable act (p. 332). However, if a person is assigned poor credit ratings because of her/his ethnic name, then it is an unfair discrimination and a biased one (ibid). However, this study claims that algorithmic systems are complex, and it can be difficult to explain why a person is denied of credit or if it was a rightful decision. It can be difficult to point out and explain the outcome, as there can be bias in data-set, data collection, interpretation of the data or in the output which can be implicit to interpreter.

On this subject Kate Crawford (2013) discusses that “data and data sets are not objective; they are creations of human design. We give numbers their voice, draw inferences from them, and define their meaning through our interpretations. Hidden biases in both the collection and analysis” stage important risks. Therefore, thinking on the possible bias in the system should have the same importance as the correlations algorithm found in the data-set.

So, the ethical implication is that data reflect the economic and social imbalance which may result in furthering discrimination, bias and economic shortcomings because the scoring algorithm can automatically deny credit to individuals. The report is representative of the current inequalities in the American society. That is to say, algorithm can be right to find a correlation between low income and being credit invisible or that African-Americans and Latinos are more credit invisible than White people. This may stem from the systematic discrimination towards those ethnic groups or it may reveal the economic inequalities in the American society.

It is also necessary and important to be able to explain why a credit is denied to a specific person. Burrell discusses that that in a conversation with FICO (Fair Isaacs

Corporation), they state that they try to avoid machine learning algorithms, as it is not sure what they learn and also Fair Credit Reporting Act requires that reasons must be given to people for denied credit (2016, p. 11). As discussed by Brevoort et al. in the report, "estimating the number of credit invisibles is complicated by the fact that almost no data exists specifically for this population" (2015, p. 9), referring to complications in data collection and data-set. Therefore, if data-set and data collection are biased, then algorithms will learn from the biased or deficient data, leading to biased outcomes.

2.2.1.9. Discrimination

Discrimination is one of the highly argued concepts in the discussions of algorithmic culture. The literature generally address how discrimination emerges as a result of bias in the algorithmic systems and due to decision-making feature of algorithms (Mittelstadt et al., 2016, p. 8). It is discussed that automation of algorithms and autonomous decision-making algorithms may lead to biased results, making it harder to detect bias such as algorithms that are used in hiring. Discrimination is also discussed with health data, wearable technologies that collect health information and how predictive analytics can result in discrimination such as predictions about if a person is likely to develop certain health conditions. The issue is also discussed with search engine technologies, questioning how algorithms working on search engines contribute to discriminative ad and information delivery. Another area where discrimination is discussed with algorithms is that profiling and predicting algorithms can produce discriminative outcomes, as in the examples of predictive policing. The discussion generally focuses on the fact that there is not enough transparency on the algorithmic systems, preventing human agents from gaining insight about what causes discrimination in the systems.

The case that is going to be examined is about face recognition algorithm of Google tagging black people as Gorillas, questioning morality of machine learning.

Google was criticized a lot after its image-recognition algorithm tagged two black people as "gorillas" (Hern, 2018). Why the system labelled people in this way was that training data which was used by the algorithm had very few examples of dark colored faces (Jagadish, 2016). As a result, the algorithm was not able to appropriately recognize different faces, because it was not trained or it did not learn properly to distinguish and recognize dark colored faces. What this example shows that training data can raise an ethical issue, if they are not rich and *diverse* enough, especially when working on data pertaining to people.

Crawford discuss this issue as *signal problem* referring to misconception on how people think about data: people think that data reflect social world precisely, but she argues that there are important gaps where little or no signal received from distinct communities (2013). As in our example, training data do not reflect our social world, it is deficient. It does not include enough examples of dark colored people. Therefore, it can be concluded that algorithms will be as good as the data they work on (Barocas & Selbst, 2016, p. 671; Jagadish, 2016). Therefore, the ethical implication is that if data model or training data is not inclusive, the output of the algorithm will not be inclusive, too. Thus, there is no point in blaming algorithm for the deficient outcome.

Barocas and Selbts (2016) discusses that data that are imperfect may allow algorithms to adopt prejudices of previous decision makers or biases in the society (p. 671). They further argue that biased training data results in discriminatory models (p. 680; Custers, 2013). And “if data mining draws inferences from a biased sample of the population, any decision that rests on these inferences may systematically disadvantage those who are under- or overrepresented in the dataset” (p. 681). This means that flaws in the data gets into algorithms and they are implicitly or explicitly emerging in the patterns, models and outputs of the algorithm.

This case study should also be considered with the opaque nature of algorithms which led them to be ‘black boxes’. Frank Pasquale (2015) discusses that *black box* is a metaphor which has dual meaning: first, referring to the fact that everything is recorded just like by a recording device in airplanes: second, referring to systems working mysteriously where people can see inputs or outputs, but cannot explain why (p. 3). For example, people are tracked on daily basis by companies or governments, but people do not know exactly how data are used, what consequences it will bring or how much of their information can travel (ibid). Pasquale uses the term black box when examining the effects of opaque algorithms in finance, credit and search engine rankings (p. 4-5), and he described opacity as “remediable incomprehensibility” (p.7). He discusses that this problem matters because decision-making process are now conducted automatically, lacking of human reflection: authority is manifested algorithmically: rules and instructions are computed in a matter of seconds (p. 8). Thus, he refers to the fact that we have little understanding of automated, decision-making and ubiquitous algorithms and that they are incomprehensible - opaque to us, even though they are parts of our social world.

Therefore, opacity emerges when we do not understand or have access to inner workings and rationale of algorithms: when they are complex in nature, referring to absence of technical knowledge to understand: when they are inscrutable to outsiders because of proprietary algorithms and concerns of companies about their trade secrets or their competitive advantages. Thus, opacity is about not being able to explain outputs of the algorithm, not being able to understand the logic behind the system, not having access to inner-workings of the algorithms and not having enough technical literacy to comprehend, even if proprietary algorithms are open to people.

Moreover, Jenna Burrell (2016) discusses opacity with an emphasis on machine learning algorithms and she argues opacity in three forms “(1) intentional corporate or state secrecy, (2) opacity as technical illiteracy, and (3) an opacity that arises from the characteristics of machine learning algorithms and the scale required to apply them usefully” (2016, p. 1). The first type of opacity occurs as a “self-protection by corporations” to protect their trade secrets, corporate secrecy and proprietary algorithms for competitive advantage and also to prevent their systems from manipulation and gaming (ibid, p. 3-4). The second type of opacity emerge as a technical ability and a necessary skill to understand, read and write code and to implement algorithms. However, it is discussed that a big part of the population will still be illiterate and will not understand, even if code transparency is ensured (ibid). The third type of opacity centers on “mismatch between mathematical procedures of machine learning algorithms and human styles of semantic interpretation” (p. 3). This means that machine learning algorithms have some “challenges of scale and complexity” in relation to number of “pages of code” and number of teams working on the system, “multitude of interlinkages of modules and subroutines”, understanding the algorithm working on data and learning aspect of machine learning (Burrell, 2016, p. 5). As a result, these complexities specific to machine learning algorithms result in opacity.

However, this opacity can be even opaque to their creators. That is to say, outputs of the algorithm can be in a way that even “the human trainer himself is unable to provide an algorithmic representation” (Matthias, 2004, p. 179). Therefore, code transparency and audit can be a response to scrutiny, but they are also challenged with complex output of algorithms which are even incomprehensible to its developers.

As a result, considering the fact that Google’s image recognition is a machine learning, Google’s algorithms are proprietary and the challenges specific to machine learning, it can be discussed that algorithms may have bias or discrimination as a result of their opaque nature. It can be concluded that there are two ethical problems in this case: biased data may result in discriminatory results: and, opacity complicates why algorithm produces the output it produces. In that sense, they are powerful agents with ability of affecting individuals and groups in the society, creating a cultural significance.

2.2.1.10. Automation

Automation of algorithms and the ethical implications of automation is a highly discussed subject. However, in this thesis, automation will be inspected in relation to creation of inequalities which is a conceptualization of Virginia Eubanks.

Algorithmic automation is described as “a potent form of social engineering, capable of vastly expanding and accelerating our capabilities for interpretation, organization, and production” (Lowrie, 2018, p. 356). Thus, there is a strong belief that automation of algorithmic system will increase our capacities. According to Paul Dourish, the relation between algorithms and automation refers to “a system of digital control and management achieved through sensing, large-scale data storage, and algorithmic processing within a legal, commercial, or industrial framework that lends it *authority*[66]” (Dourish, 2016, p. 3) Therefore, it refers to a “regime of computer based monitoring and control” and algorithms play an important role in the “expansion of sorts of regulative,

---

[66] Emphasis is added.

coercive, and divisive processes” (ibid) such as in political systems, financial systems, public surveillance, employment, credit scoring, health and etc.

Thus, it can be seen that automation of algorithms refers to a change where decision-making and control are given to algorithms and to algorithmic systems from human agents. The general belief is that potential of data and algorithms will make better decisions than human agents. However, literature questions shifting augmentation and automation of knowledge work from humans into algorithms (Naik & Bhide, 2014, p. 51). Also, when decision-making processes are assigned to automated algorithms, then ethics of automation emerges questioning agency and responsibility of the automated agents. This study asserts that automated systems can create unfair and biased results which can create new forms of inequality reflecting the inequalities in the society. We will now examine a case study where automated hiring system creates inequality for the potential candidates.

When hiring people, companies would like to make use of the capacities of the data. In order to calculate the likelihood whether a person will stick to the job, the company Evolv helped the company Xerox to provide them with more efficiency for their hiring process (O’Neil, 2016). It is because replacing employees causes extra money for the company and it means loss of efficiency. Therefore, they wanted to figure out some metrics to help them select the right people. One of the emerging correlations was candidates’ geography. The correlation took commuting times of the employees into consideration. The longer the commuting time is, the more likely the employee performs poorly or it even results in quitting (ibid). However, the company Xerox soon realized that there was another correlation. Most people who commute long were also from poor neighborhoods (ibid). As a result, the algorithm was blocking the way for poorer people to be considered as candidates when they applied for a job. Although this was unintentional, the algorithm automated inequality and it was unethical by design. After realizing this outcome, Xerox removed the correlation on geography from their model for the sake of fairness (ibid).

Thus, the implication is that we are living in a world which is populated by data and whose main input is data. It constitutes the main drive in information societies. Therefore, when a company wants to search for a new candidate, it is sensible to employ algorithms to make sense of it, because algorithms have the capacity of processing more data in a shorter time period than humans, bringing efficiency. However, as discussed here, it can bring unfair and biased results and create new inequalities or it can emphasize the inequalities that is available in the society. Virginia Eubanks calls this situation *digital poorhouse* which is “the sort of invisible institution that’s made up of decision-making algorithms, automated eligibility processes and statistical models across a really wide range of social-assistance programs” which arises because of the USA’s concept of poverty and their social assistance system which is punitive (Young, 2018). However, it can be possible to experience inequalities of automated systems in anywhere.

The ethical implication is that automated algorithms can result in unintentional inequalities. However, it is believed that algorithmic decision-making can be more pervasive than human decision-making and can be better at hiding it because of their complex nature.

2.2.1.11. Commercialization

Commercialization is this thesis’s own conceptualization as an ethical problem rising from features of algorithms and related practices, claiming that algorithms used for user profiling and tracking on OSPs with economic incentives such as targeted ads result in commercialization of information, search, behavior and conduct.

Information societies are full with data and it is not always easy to categorize necessary information or it is not always possible to differentiate the noise from data or understand the line between information and knowledge. For this reason, profiling is actually an important technology to save information society from its two distinct problems which are overload of information and blurred borders of information, knowledge and noise (Hildebrandt, 2006, p. 548). Therefore, profiling allows us to separate data as relevant and irrelevant, turning data into information which then results in creation of knowledge (ibid). Thus, it can be deduced that profiling is about knowledge, not about data.

As Hildebrandt and Koops (2010) discuss that profiling is not only efficient in organizing and processing information and data, but it is also efficient in terms of time, energy and attention, as they have more developed capacities than human beings (p. 431). However, in spite of the capacities of profiling which bring efficiency, when profiling is used for commercial incentives and surveillance aims, it can also be a tool for abusing citizens, consumers and users.

Then, what is profiling? Profiling is a term that is actually used for pattern recognition (Hildebrandt, 2006, p. 548). And, profiling which is conducted by algorithms is defined "as the construction or inference of patterns by means of data mining and as the application of ensuring profiles to people whose data match with them" (Hildebrandt & Koops, 2010, p. 431). Thus, profiling happens when algorithms create meaning and patterns from data by data mining and then matching people's data with the created profiles. When talking about how profiles are matched with people's data, there is also a 'persons vs profiles' situation that needs to be mentioned. While the 'persons' is about personal data and "individual pieces of information", the 'profiles' is about "model correlations between pieces of information appearing in individuals' data, casual patterns and general rules that apply to a subset of the individuals" (van Otterlo, 2013, p. 43-44). That is to say, persons level is information related to personal data, but profiles level is about correlations between the information in the patterns which are applicable to groups of individuals.

Thus, the other thing that needs to be asked is how profiling is done. Automated profiling is conducted on different phases: recording of data (making real world situations machine readable), storing of data (making it accessible, aggregated), tracking data (enabling linking data to the same subject), finding patterns in data (data mining, application of algorithms on data) and monitoring data (verifying if new data confirms / fits the pattern or correlations) (Hildebrandt, 2006, p. 548-549; Hildebrandt & Koops, 2010, p. 431-432). Thus, it can be concluded that profiling happens by taking real life situation and turns them into machine readable forms, identifying patterns in the data and linking with the data subject and checking if new coming data fits into correlations.

Therefore, when we say data, it is about every piece of information in the database, but when we say profiling, it is about user data -consisting of pieces of information allocated to same entity- and also user behavior such as a person's click behavior on a webpage (van Otterlo, 2013, p. 43). That is to say, profiling is about behaviors of users. We will now examine an example of behavioral profiling and tracking which resulted in behavioral targeting.

A person was searching for articles on Google search engine about handling stress and overcoming procrastination. She visited variety of web pages and scrolled through the articles in expectation of helping herself. The next day, when she visited the Quora which is a question and answer website to read an answer for a completely different question, the website offered her to click on the headline "three ways to stop procrastinating". She clicked on it fast just to find out that it was a paid psychological help package. How did Quora know that she was the queen of stress and procrastination lately and she was searching for help to end her stress and procrastination? So, what was happening here? The thing was that Quora was somehow able to know about her previous searches on Google and was able to show her ads about what she exactly needed.

This case was possible because of *tracking*. Tracking happens during data collection stage and during linking data to the data subject. As discussed by Claude Castelluccia (2012), a big part of information which is used to profile are obtained from web tracking such as tracking people through their visits to various web sites and pages (p. 23). The reason why companies are able to build profiles of users is thanks to their tracking practices. And, Google is one the most important platforms among OSPs thanks to its large-scale data collection and its capacity of user profiling. Profiling is important for companies, because it creates value, meaning and knowledge which will be later used to customize their services according to their users' preferences. This is of course conducted to gain more profit. As in this case, the reason why she received targeted ads was that Google was able to track her search queries and build profile related to her interests. It was then marketed on Quora as targeted ads thanks to behavioral targeting.

The ethical implication of the study is that algorithms that are used for profiling and tracking can become tools for companies to target users with ads in order to gain profit. Thus, it is believed that profiling will result in more customized advertisement which will result in more commercialization. This is because users will have what they look for even before they demand it. And, as a result of this customization, it is argued that search queries which are even about personal and private issues such as health and psychology will become an object of monetization and will become companies' playground of persuasion. The basic need for information will be commercialized.

2.3. REGULATORY RESPONSES[67]

In algorithmic culture, the work of culture is assigned to algorithms and the work of humans is given to computing systems more and more (Striphas, 2015). As a result of this, humans and computers are interacting, working and creating consequences of technologies together more than ever before. Within the framework of this study, it was previously discussed that decision-making, autonomous, learning, prioritizing, micro-targeting, opaque and gate keeping features of algorithms are creating various ethical problems such as invasion of privacy, discrimination, bias, automation, ossification, manipulation, asymmetry, data ownership, commercialization, consumerism and appetite of consumption. These problems were discussed with case studies empirically to reveal their impact on social life and cultural field. And now, this study asks what will be our (users, technologists, police makers, decision makers etc.) action in the face of these challenges? What should be the response to handle these ethical issues? This study frames and suggests four regulatory responses to address these challenges, impacts and harm caused by algorithms. The responses are accountability, transparency, notification and direct regulation of governments and institutions. In this part of the study, these responses to ethical problems will be discussed and the stance of the thesis will be argued afterwards.

2.3.1. Accountability

The first response is about sparking a debate on accountability which is considered as a precondition of the remaining regulatory responses or as the base of every regulatory response. This is because we are living in modern information societies where most part

[67] This title is inspired by Tüfekçi et al.'s article called "The ethics of algorithms: from radical content to self-driving cars".

of our lives are computerized and most of our doings are conducted by computers. This means that our lives also have become more open to problems experienced in technological systems. In other words, the increasing application of computerized systems into mundane life has excessive implications which may lead to various risks or harm. Therefore, accountability for the harms caused or the possible future risks is an important response.

As discussed by Helen Nissenbaum (1994), accountability is a “powerful tool for bringing about better practices, and consequently more reliable and trustworthy results” which means that “there will be someone, or several people, to answer” for the problems (p. 74). If there is no accountability for the negative outcomes of the technology, then it means there is nobody to answer the risks or harms. And, the harms caused by the technology will only be discussed as unfortunate mistakes which would only be considered as results of brave new technology (p. 73). She discusses that there are four barriers to accountability which are listed as problem of many hands, bugs, computer as scapegoat and ownership without liability (p. 75). She argues that when there are many people creating a system, assigning responsibility on a single person or identifying who is accountable is difficult, because it is not easy to generalize responsibility to collective action (ibid). Even for bugs, she argues that there should be accountability (p, 77). She states that the reason why people treat computers as scapegoat is because computing systems are considered as mediators of interactions between humans and machines which results in distancing human actions from their results, making it easier to blame the computer system for the harms (p. 77). She further criticizes that software industry claims maximum property ownership and protection, but denies accountability as much as possible (p. 78). These four barriers function for the purpose of the study and it is important to realize that concepts of accountability and responsibility are firmly intertwined with each other. It is claimed that responsible behavior increases accountability. And, if responsibility is not accepted in the face of harms, mistakes, malfunctions, problems and future risks, then it will mean breaking down of accountability.

Then, it can be questioned what it means for algorithmic systems to be accountable? What does algorithmic accountability imply? Nicholas Diakopoulos discusses that algorithms applies power in decision-making processes such as filtering information, classifying or prioritizing (2015, p. 402). However, this thesis argues that what allows algorithms to filter information or classify things is not power, but capacities of the algorithms. He further states that apart from these algorithmic influences, there are human influences in algorithmic systems such as selection of training data, interpretation of results or criteria of choices (ibid). As a result of this, he argues that algorithmic accountability needs to consider algorithms as output of human creation and should question the intent of the creator, understanding that individuals or groups of people may have been influential in design process and human agency in interpreting the results of the algorithm (ibid). Therefore, when we discuss algorithmic accountability, it means discussing outputs of algorithms resulting from their capacities and also human effect on these systems.

One barrier to algorithmic accountability is defined as *accountability gap* by Beatriz Cardona (2008) which refers to the gap "between designer's control and algorithm's behaviour" (as cited in Mittelstadt et al., 2016, p.11). This definition is used to describe situations where responsibility or blame can be given to more than one moral agent at the same time (ibid). This can be applied to situations where groups of people contribute to a system and there is a distributed responsibility, blame and morality. However, the conceptualization of accountability gap is also used in this study to refer to situations where output and behavior of algorithms differ from the design and intent of the designer. In other words, it refers to cases where designer cannot foresee the potential risks and the system creates harmful outcomes. It is about unexpected results. It is believed that if the algorithm differs from the intention or design, there happens to be an accountability gap. However, companies, creators, engineers or designers should still be accountable for the unexpected outcomes or potential risks for their creations, but this conceptualization is adopted particularly to refer to situation where outcome and intent differs from each other.

To sum up, accountability is considered as the base of every regulatory response, because it provides responsibility for the outcomes of the technologies, it creates a responsibility area for everyone in the algorithmic system. Algorithmic accountability is discussed as a mixture of human and machine influence. Even though there are several barriers to accountability such as “many hands, bugs, computer as scapegoat, ownership without liability” (Nissenbaum, 1994, p. 75) and accountability gap, it is important to own the outcomes, to take on and distribute responsibility in these technological assemblages. Otherwise, it would mean breaking down of accountability which will potentially result in more dramatic risks and harms.

2.3.2. Transparency

Transparency as a regulatory response has some complications and it is not an ideal that can be achieved. However, it opens up important ethical discussions and poses questions that are essential for the study.

Why transparency is desired? Transparency is desired for algorithmic systems. One reason is that outputs of algorithms could be hard to predict or explain (Tutt, 2016, p. 102) which would result in difficulty to correct or control the algorithm (Mittelstadt et al., 2016, p. 6). Second reason is that opaque nature of algorithms makes it difficult for people to understand the rationale of any algorithmic outcome and it will be hard to tell whether algorithm is misused or not (Tüfekçi et al., 2015, p. 11). Algorithms working like black-boxes produce subjective decisions which may involve implicit or explicit biases (ibid). Thus, the call for transparency aims to solve this problem – to reveal how algorithms operate behind the curtain (Seaver, 2014, p. 7). The argument states that if people know the details of the system better, people can engage in critiques more effectively which will result in better algorithmic design (ibid). Third reason is the increasing lack of human accountability, meaning that the concepts of power and authority is shifting from people to machines which makes algorithmic transparency an important challenge for the time period we live in (Rainie & Anderson, 2017). In this situation, not only humans are freeing themselves from responsibility, but also understanding outcomes of the algorithms are challenged with their capacities.

Where transparency is needed? Transparency is demanded in different areas and at multiple dimensions such as transparency over data, code, algorithm and models used. Transparency of inner workings of the algorithmic systems. Transparency for the outputs. Transparency for institutional processes. Transparency of companies or platforms which collect, store, operate and make use of data.

When transparency is ensured as an ideal, it is thought that it will be possible to understand why an algorithm produces a particular output. Users will have more control over the process by knowing how companies program, how algorithm work and how their data are used. People will be able to eliminate the creepy factor, in a sense. It is argued that disclosing information will lead to reduction in information asymmetry (Diakopoulos, 2015, p. 403). Transparency is thought to offer “a way to see inside the truth of a system” (Ananny & Crawford, 2016, p. 2). Therefore, the assumption is that seeing will mean understanding and will create obligations for accountability which will be followed with *change* (ibid). In other words, observation will turn into knowledge which is to be used to govern and make systems accountable (ibid). Thus, transparency is no longer just a state where anything is obvious and exposed, but it is a system of observing and promising control to users (ibid, p. 3). Also, as transparency will make systems open to scrutiny, it is believed that transparency can also prevent discrimination or biases in the system, because everything will be apparent to related parties (ibid, p. 5). Therefore, it will not be wrong to deduce that transparency is often considered “as a panacea for ethical issues arising from new technologies” (Mittelstadt et al., 2016, p. 6). However, oftentimes this idea is challenged and transparency is considered as a failed response to algorithmic regulation. Before explaining why, it is first needed to ask what transparency exactly is.

What is transparency? According to Turilli and Floridi (2009), transparency is related to “availability of information, the conditions of its accessibility and how the information, which has been made transparent, may pragmatically or epistemically support the user’s decision-making process” (p. 106). This discussion is not a new one. While information/business ethics describes transparency as “forms of information visibility” and “possibility of accessing information, intentions or behaviours that have been intentionally revealed through a process of disclosure”, computer science defines transparency as “a condition of information invisibility” (ibid, p. 105). So, while the former one describes it with the process of disclosure, the later describes it making computing process transparent. They further argue that transparency is “not an ethical principle in itself but a pro-ethical condition for enabling or impairing other ethical practices or principles” (ibid). This means that transparency is a condition that works with other practices and principles, but it does not create an ethical principle on its own.

What are the primary components of transparency? Primary components of transparency are described as "*accessibility* and *comprehensibility* of information" (Mittelstadt et al., 2016, p. 6). This means that information that is made transparent needs to be accessible and comprehensible, because transparency is not an enough condition for an ethical response. Imagine that inner workings of an algorithm are transparent, meaning that it is open and available. However, it will not be meaningful or useful, if it is not comprehensible or if it is not accessible to interested people.

Why is transparency considered as a failed response? Transparency is considered as an ideal that has failed. Challenges to transparency will be discussed to understand better what is needed to make it a functioning response. It would be better to start with the idea why a person should search not only for information, but also for the visibility of that particular information, s/he can understand the visible –the obvious- with the ability of evaluating and interpreting the apparent information and finally s/he can decide its importance in the system (Ananny & Crawford, 2016, p. 7). These traits attributed to a person are the result of enlightenment which leads to a "belief that putting information in the hands of the public will enable people to make informed choices that will lead to improved social outcomes" (Schudson, 2015, p. 22 as cited in Ananny & Crawford, 2016, p. 7). Therefore, there is an opinion upheld claiming that transparency will make information accessible and comprehensible to the public, and the public will be able to understand them and they will be able to make choices in accordance with the information that is made transparent to them and this will lead to better social results. However, there is one idea which breaks down this whole narrative and it claims that *seeing is not equal to understanding.*

Therefore, the first challenge to transparency as a regulatory response is that seeing is not equal to understanding. Seeing inside of a system does not guarantee understanding a system's behavior or its origins, because without comprehensibility seeing itself does not function (Ananny & Crawford, 2016, p. 8). Also, looking inside of a black box is found as a limited and an ill-fitting metaphor for the complex problems of algorithms, because seeing comes with its own ideological complexities (ibid, p. 10). And, it is important to note that knowing something does not emerge from looking into something (ibid), but it rather emerges from understanding.

Also, revealing source code of an algorithm is discussed for transparency (O'Neil, 2014) and that it will enable algorithmic transparency and will result in better understanding of the inner workings of an algorithmic system. However, it is argued that allowing access to an algorithm's source code does not mean that it will ensure scrutiny (Tüfekçi et al., p. 11), ethical behavior (Mittelstadt et al., p. 13) and effective user experience (Diakopoulos, 2015, p. 411). It is generally discussed that revealing source code will be helpful for technologists or people who have enough technical background to understand the inner workings. The belief is that they will eventually make more insightful decisions and evaluations. However, revealing source will not be useful for public who lack of technical capacity. Even though this claim is partly correct, this idea is also challenged with the fact that there are times when even engineers who develop the system cannot understand the outputs of the algorithmic system. In other words, it is also possible that people with technical capacity and expertise may not understand the output, in spite of transparency over source code and inner workings.

Therefore, the second challenge to transparency as a regulatory response is that *technical capacity may not ensure transparency*. There will be technical limitations of understanding even for engineers, designers or technologists. Nick Seaver (2014) discusses that by assuming that engineers have a total understanding of their creations, people make two mistakes: the first one is that algorithmic systems are products of many hands working with different goals and the second one is that it can be difficult to predict the outputs of an algorithmic system, after it has a level of complexity (p. 8). Therefore, revealing source code or inner workings of algorithm assumes that these systems work clearly (ibid), and they will not produce unpredictable results. However, even engineers may not easily understand the logic or rationale behind these systems, because of "scale and speed of [their] design" (Ananny & Crawford, 2016, p. 9; Burrell, 2016) and machine learning making decisions that are not programmed (Tüfekçi et al., 2015, p. 11). Thus, revealing how an algorithm works is insufficient even for developers, because it assumes that output of the system is predictable. It ignores the fact that machine learning can create results that are not programmed and it misses that there are many people working on these systems, increasing the complexity of understanding these systems.

Talking about the technical aspects of transparency and its limitations, the third challenge is *functionality.* It is discussed that even if source code, training and testing data set are revealed, code/data made apparent may only give a "snapshot of its functionality", as they are changing and learning structures (Ananny & Crawford, 2016, p. 10); and it may still not be possible to ensure transparency, because the code made accessible can be different than the source code in operation, meaning that there could be a *versioning* complication (Diakopoulos, 2015, p. 411). Thus, transparency has not only ideological, but also material and technical challenges.

Even though transparency may sustain accountability, *full transparency* can also cause harm. If transparency is implemented without thinking comprehensively why, how and which parts of the system should be made transparent, then it can be a factor that triggers harm in so many aspects (Ananny & Crawford, 2016, p. 6). It can result in loss of privacy, it can pose individuals or groups of people open to bad intentions, people can be a subject of power and it can create power asymmetry. Full transparency can be harmful not only for companies themselves, but also for their users. However, when the issue is transparency of companies, even little transparency over their proprietary algorithms can cause various harms. And, companies will not be eager to open their proprietary algorithms to public, because it will mean revealing a lot of details about their work which may put them in a vulnerable position. Problems that may arise are generally listed as: concerns about trade secrecy, systems being exposed to manipulation/gaming, damage on corporate reputation, issues on security and inefficiency of transparency.

It is discussed that when companies expose proprietary algorithms, the fear is that it will give away their trade secrets and damage their competitive advantage, so companies limit their level of transparency (Diakopoulos, 2015, p. 403). Also, what companies grant access on may hurt their reputation, because their inappropriate activities will be the attention of scrutiny, affecting their ability to perform business (ibid). However, public access to algorithms may also put companies in an open position where users or parties can use it as a chance to game, spam and manipulate the system (ibid; Tüfekçi et al., 2015, p. 11; Crawford, 2016, p. 87; Granka, 2010, p. 366; Seaver, 2014, p.7). Transparency can also be a threat to the commercial survival of data processors such as credit reporting or high frequency trade (Mittelstadt et al., 2016, p. 6). As a result, it can be concluded that transparency of proprietary algorithms is controversial with regards to competitive advantages, trade secrets, security, privacy and manipulation.

Apart from commercial concerns over transparency, there is a never-ending tension when governments use algorithms and when they try to decide how transparent their systems, works and conducts will be. The tension is generally exacerbated with the trade-off "between transparency and national security" (Diakopoulos, 2015, p. 403). Even though, the trade-off on transparency generally hides behind the concerns of security, it tends to be more about politics.

Another point that challenges transparency is that a "complete documentation takes time and money" (Tüfekçi et al., 2015, p. 11). In other words, transparency is not a practical ideal to be achieved.

To sum up, applicability of transparency is challenged with four different perspectives: seeing is not equal to understanding, technical capacity may not ensure transparency, functionality and full transparency can cause harm. However, it is believed that transparency as a regulatory response should not be abandoned, but shifted.

How should we understand transparency as a regulatory response? It is discussed that transparency as an ideal cannot be achieved and it is not a sufficient regulatory response, as argued above. However, this does not mean that thinking on transparency does not open up the field. If perspective on transparency is shifted, then it is believed that it can pose more responsive questions.

According to Ananny and Crawford (2016), the aim of transparency needs to change. We should not look *inside* the system, but we need to look *across* the system, when the system is not a "positivist discovery", but it is a "relational achievement among networked human and non-human agents" (p. 11–12). Why we should look across, instead of inside stems from the fact that significance of human and non-human agents "lies not internally but *relationally*[68]" (ibid, p. 12). In this study, algorithmic systems are considered as socio-technological assemblages where humans and non-humans interact, work together and affect each other. Therefore, transparency cannot be achieved by

[68] Emphasis is added.

looking inside, but by looking across the relations between distributed actors. This can bring insights.

Transparency without comprehensibility is meaningless, ineffective and it is not functioning. Therefore, one idea can be that transparency can be more impactful and effective, if disclosure is not directed towards subjects, but towards regulators who will inform the public about the implications and who will represent public interest (Mittelstadt et al., 2016; Zarsky, 2013; Zarsky, 2016). In this way, it is believed that transparency can function and will be more accessible by data subjects, too.

2.3.3. Notification

Notification as a regulatory response is generally discussed as a supporting and distinct form of transparency. Tüfekçi et al. argue that consumers should be able to control their own personal information which is given to algorithms, because it may have important influence on people’s lives (2015, p. 11). According to their conceptualization, the control over personal information includes two points. The first point is about having “rights to correct information” and the second point is about demanding “personal information to be excluded from database of data vendors” (ibid). This means that users should have rights to correct information about them on online or in databases. It can be as simple as correcting a demographic information about themselves or it can also be wrong information which may harm their reputation and sociality. Similarly, people should be able to demand their personal information to be removed or excluded from the Internet and databases, because personal information can reveal too much about a person’s life and result in loss of privacy.

In addition, the thesis suggests that notification can be regulated in four different ways: opt in and opt out options, graduated choices, full notification and simplified choices. The first one gives users choice to opt in or opt out for applications that they consider inappropriate. This is about giving users some degree of control over their choices against companies’ top down practices. The second suggest that users should have graduated choices when they agree to use platforms or websites. That is to say, privacy policies or “I agree to use” buttons can be designed in a way that offers graduated choices to users, asking if they want tracking cookies, if they want their data to be used for targeted ads, if they want personalization for the sake of relevancy and etc. This can ensure agency of the users, provide input of the users in technological assemblage, prevent unwanted intrusive outcomes and abandon all or nothing approaches. The third one is full notification which means informing users comprehensively when platforms or companies make use of their data. It asserts that users should be fully notified about which data, for which purpose and how will be used. The fourth is simplified choices. This criterion suggests that when companies make amendments to agreements and privacy policies or when users sign up to platforms, users should be given simplified choices to understand the alterations in the agreement and should have a simplified design to decide which default settings they would like to comply with. In this way, it is believed that the interactions between human, machines and companies would be clearer, healthier and more direct, diminishing the unexpected results and ensuring a more open communication.

2.3.4. Direct Regulation of Governments and Institutions

The fourth response *direct regulation of governments and institutions* is developed for the emerging problem that self-governance of companies with ethical principles is falling short and that we need better oversight, governance and control over private companies' practices with data-driven algorithms to regulate them better.

New AI Now report suggests as one of their recommendations for the future of AI that "governments need to regulate AI by expanding the powers of sector-specific agencies to oversee, audit, and monitor these technologies by domain" (Whittaker et al., 2018, p. 4). The point they argue is that national safety bodies or general standards over AI will not be practical to have a nuanced regulation, and they offer a sector-specific approach which focuses on the application of technology in its domain (ibid). The second point they argue is that AI Now 2017 report has previously supported the idea of ethical codes, as well as oversight and accountability mechanisms (p. 29; Campolo, Sanfilippo, Whittaker & Crawford, 2017). They reveal that even though there were companies rushing to adopt these kinds of codes which mainly addressed the discussion around design and implementation of AI, there was not a strong accountability or oversight to support such ethical efforts (ibid).

They argue that equitable systems need more than ethics itself, because it is seen during the year 2018 that there is an increasing accountability gap. Also, there were many scandals such as manipulation of users and citizens in the examples of Cambridge Analytica and Brexit. These scandals were exemplifying how ‘well-intentioned’ promises of companies were ineffective. Lucy Suchman discusses that companies’ ethical principles such as “Don’t Be Evil” or “Do the Right Thing” are remaining “vacuous … in the absence of the requisite bodies for deliberation, appeal, and redress” (2018). It is discussed that these kinds of “trust us” ethical promises of the companies are reaching nowhere that is ethical. In this respect Ben Wagner discusses that ethics is “unable or unwilling to properly provide regulatory solutions, ethics is seen as the ‘easy’ or ‘soft’ option which can help structure and give meaning to existing self-regulatory initiatives” (2018, p. 1). That is to say, ethics is seen as a way to accept that there are problems existing, without having enough power to regulate or affect the way technology is implemented by companies and technologists (AI Now, 2018, p. 31). In this sense, it is argued that we cannot trust companies to implement ethics, we cannot expect them to be ethical in their self-governing practices. Thus, ethics is seen as deficient in meeting the needs for accountability. The report suggests that external oversight which would check, control and balance the accountability of companies is necessary, but we also need ethical cultivation of norms and values both in the companies and in professions (p. 32). Therefore, the report argues that ethics is understood by companies as promises which can be broken easily without any enforcement following their bad practices and they suggest for stronger enforcement to be implemented by governmental bodies which would not be so easy to breach and break.

Besides, Tüfekçi et al. (2015) discusses if some algorithms such as high-speed trading algorithms and search engine algorithms should be regulated more directly (p. 12). That is to say, direct regulation can focus on practices of companies and technologists, but it can also focus on algorithms, too. For instance, they ask “can regulators require Google to force its algorithm to act in certain ways towards certain competing sites” (ibid)? However, direct regulation on algorithms is found problematic for a few reasons: it would require access to proprietary algorithms of companies which would possibly never happen: modifying algorithms for public interest would not be possible, because the understanding of public interest is subjective – there is no standard of it: and it is not possible to predict the output of the algorithms in an exact and objective way (ibid).

The stance of this thesis on direct regulation of governments and institutions as a regulatory response is that it is necessary to have external bodies to control conducts and practices of private companies. AI Report suggests governmental bodies and institutions to close the accountability gap and to create oversight over practices. However, this thesis thinks that it is also important to ask these questions: who would control, check and create balance for the practices of governments? How can we be sure that intuitional mechanisms are not biased and what would be the transparency steps in order to close the accountability gap – pertaining not only to companies, but also to the accountability gap within the governmental bodies? In others words, who would bring ethical oversight, external enforcement and control on governments' practices with data driven algorithms? Also, how could we define public interest? How can we develop standards for it? It was discussed that 2018 was the year of scandals. However, this study understands that the reason why ethics stay as a "soft" solution is that ethical flourishment does not come within the society, it is more discussed within the institutions or by groups of people concerned about the situations. However, it is thought that even though 2018 was the year of scandals, the society is not responsive enough to force ethics. Because ethics is bound to culture and society. If ethical idea is disconnected with the society, then it is inevitable for 2018 to be the year of scandals and we would need stronger enforcement other than the ethics itself. In other words, maybe the ethical thinking is not cultivated enough in the society to lead to more ethical results and to critical thinking over unethical practices of companies. The last point is that it was discussed that there were companies or parties that rushed to adopt, accept and implement ethical principles as codes of conducts. However, this study questions how well technologists within the companies are able to understand ethical thinking and how well they understand the problems in the society. The tension between security, ethics and concerns for profit in companies is a difficult one to tackle. The thesis suggests that we need to find ways for ethical cultivation to develop in the members of the society, technologists and in the companies, if we want to live in more ethical societies. We need to sustain interoperability of the three, as much as we need external enforcement in the forms of regulations, codes of conducts and law.

2.4. CONCLUSION OF THE SECOND CHAPTER

In the second chapter of this thesis study, an ethical discussion is started as a suggestion, response and solution for the possible ethical problems rising from the features of algorithms and related practices. It is argued that an ethics discussion will be the answer for the concern of ‘what we should do’ against unethical practices of companies and governments employing data-driven algorithms. Apart from the theoretical discussions, an ethics map is created to address ethical problems, features of algorithms and types of algorithms. At the end, regulatory responses are framed to show what kinds of actions people can take for the unethical data practices of governments and companies and for the negative impacts of the algorithms.

It is found that deontological, teleological and virtue ethics approaches can constitute the basis of the ethics discussion in the study and they are found workable. They provide technology with codes of conduct, reflections for the outcomes and the traits technologists should have for ethical thinking to flourish. However, it is also found that there are more complex problems in algorithmic culture that requires different ethical perspectives which should be more responsive to dilemmas of information societies. These problems are defined as *hyper connected* and *networked* power relations, *concept of agency, knock-on effects, knowable outcomes, unstable nature of algorithms* and *the problem of many hands.* It is argued that data ethics is comprehensive enough to tackle with these problems and it is inclusive of both data, algorithms and related practices of these two. Thus, it is concluded that data ethics is a working structure that is applicable to ethical dilemmas in algorithmic culture.

Furthermore, meaning of an ethical algorithm is discovered by questioning morality, intentionality and agency of algorithms to find out if we can hold them accountable and responsible for the unethical practices or for the disparate impacts. It is concluded that it is meaningless to blame algorithms for the emerging problems and considering computing systems as scapegoat. Because it is inferred that algorithms cannot possess the adjectives which belong to human-beings. They are reflective and responsive of the biases that already persist in the society, individuals, design, data set and data collection. Therefore, it is concluded that algorithms and machine agents can have *functional moral responsibility* (Dodig Crnkovic & Çürüklü, 2012) for their *regulatory* *role* in the assemblages where responsibility is understood as a distributed and network concept. However, on the accountability dilemma, it is concluded that companies and individuals who develop technology and who pursue economic incentives should have a bigger responsibility from this discussion and they should own the outcomes of the technology they develop.

On the ethical approach of this study, several perspectives are adopted. H.V. Jagadish's approach of 'ethics are practical, regulations/laws are not', 'do not surprise data subject and own the outcomes' are found suitable for the purpose of this study. Ladikas et al.'s perspective of 'we cannot separate ethics from cultural/social norms and values' and 'ethical ideas pave the way for policies' are the second perspective that is found compatible. And, Annette N. Markham's approach of impact model is found relevant for developing reflections for the possible outcomes and pitfalls in the development of technology. This thesis's own approach nourishes from the previously discussed approaches and concludes that there cannot be a single approach to be adopted, because ethical problems are diverse and there is no standard of them.

For the emergent problems, regulatory responses were framed that have been already discussed in the literature as *accountability, transparency, notification* and *direct regulation of governments and institutions.* The stance of this research is that we need regulatory frameworks, institutional bodies or external structures to control and check practices of companies on data and algorithms, but we also need ethical thinking. It is concluded that we actually need ethical thinking in the first place. Because it is thought that the force which comes from regulatory bodies will remain artificial, but the force that comes within the society is an organic one and it has the power to make companies and governments insightful about their actions. Because governments would not want citizens to be their opponents and companies would not like to lose their users who bring them profit. Thus, they have to compromise. This is the power that is found in flourishment of ethical thinking.

Ethical cultivation is not only necessary for the society, but also for those people who develop technology. It is found that we cannot develop technology for the society, if we do not understand the society, its problems and dynamics. Thus, ethical cultivation is not regarded as a soft power, it is a power that can be achieved only when it is adopted by the different parties in the society which will lead it to become like synapsis in the brain. It will start to communicate, get stronger and it will eventually become a force own its own leading to more ethical results.

The last statement of the chapter is that what would happen if we do not develop ethics? What are the things that are so Orwellian and that this thesis study is so anxious about? The case studies are indicative that if we do not take an action, invasion of privacy, commodification of personal data and commercialization of habits, beliefs and thoughts will be abused more in the future. A culture that does not confront is obliged to misconduct. Also, technology is fast paced, this is why this discussion is so urgent. A society which does not question the unethical will normalize the unethical. When unethical is stabilized, then there would be nothing to discuss, because it will not reach to society, it will not have the importance and concern for the members of that society. This is why, this thesis suggests data ethics for the emerging problems that we face now and later.

2.5. EVALUATION

This part aims to make a general assessment of the chapter, emphasizing approach of the study for discussions and providing points to connect it with the conclusion.

An ethics discussion has been started for the problems that are experienced in algorithmic culture. It is discussed that these problems were not only emerging from the features of algorithms, but also from the unethical practices of governments and companies on data-driven algorithms. Thus, ethics discussion is suggested as a solution for disparate impacts of the algorithms and for the unethical practices by individuals and corporations.

For the ethics discussion, three ethical approaches were found workable as being deontological, teleological and virtue ethics approach. They are considered as constituting the basis of the codes of conducts, responsibility for the outcomes and traits that developers should have. However, it was emphasized that in algorithmic culture, there are more complex problems that requires a more comprehensive approach which can tackle specific problems such as the issue of many hands and unstable nature of algorithms. Thus, data ethics is found to be comprehensive enough to handle these problems, as it includes both data, algorithms and relevant practices. Apart from that, meaning of ethical algorithm is discovered by emphasizing that algorithms can only have a *functional moral responsibility* (Dodig Crnkovic & Çürüklü, 2012) in socio-technological assemblages due to their regulatory role. For the ethical approach of this study, studies of Jagadish (2016), Ladikas et al., (2015) and Markham (2018) are adopted and upheld. And, the thesis is on the opinion that we cannot suggest a single ethical perspective, when problems are diverse and when there is no standard of the problems.

Apart from the theoretical discussions, an ethics map is created to frame problems, features and types of algorithms. The map is found as working, as it was able to discuss different case studies in relation to types and features of algorithms. And, problems rising from the features of algorithms were determined as *invasion of privacy, discrimination, bias, automation, ossification, manipulation, asymmetry, appetite of consumption, data ownership, consumerism* and *commercialization.*

Regulatory responses were framed to show what kinds of action people can take in the face of emerging problems. These responses were *accountability, transparency, notification* and *direct regulation of governments and institutions.* The stance of the study in relation to regulatory responses was that as much as external control and audit is required to ensure ethical practice at companies and governmental bodies, accountability can only be achieved with ethical cultivation in the society together with principles, codes of conducts, morals in the forms of responsibility and ethical decision-making.

In relation to this, the conclusion part will bring forward a better understanding of what it means for a society to lack of ethical cultivation and why it is needed within the companies. It will also explain why this thesis attaches a specific importance on the ethics itself and why it is so urgent. Besides, suggestions on how ethics can be sustained in the society will be given. In the end, reflections will be made on what is possibly waiting individuals in a society where the 'unethical' is stabilized. Moreover, the situation in Turkey in relation to data, algorithms, the Internet and related practices of the parties will be reviewed with examples. Finally, suggestions for further research will be given.

CONCLUSION

This thesis titled *Algorithmic Culture and Data Ethics* investigated effects of data-driven algorithms that run on social networks and on the Internet to culture and society. It more specifically looked at the different types of ethical problems that may emerge from features of algorithms and related practices as well as how these problems can be tackled. As a result, this study suggested data ethics as a solution to the possibly emerging problems.

The thesis starts with the assumption that it is the deployment of culture's work to algorithms that creates *Algorithmic Culture* (Striphas, 2015). In this respect, it suggests that in information societies, algorithms are not just used to make basic calculations, but to make more complex and subjective decisions for people, deciding what is important, relevant and best for them. Therefore, the thesis concludes by stating that algorithms work in the realm of culture, affecting how cultural practices are experienced and how everyday life is regulated. Hence emphasizing, we cannot and must not understand algorithms as consisting of merely code and data, but as socio-technological assemblages where human and non-human interacts and communicates (Ananny & Crawford, 2016). So, it is argued that algorithms are nor mere technological constraints or cold machines that operates on their own, but they are entities which have social, cultural and economic significance. Moreover, the interactive side of data-driven algorithms is emphasized: as much as we shape technology, it also shapes us.

Hence, in this thesis it is argued that data are valuable in information societies. It is argued that they are valuable, because they act as the new input which turns data into new oil or a new currency. Data are valuable and have economic value irrespective of how people feel about their own personal data. But at the same time data can also cause negative acts such as surveillance. In fact, data surveillance is real irrespective of how people understand transparency or even if they think that they have nothing to hide from their governments. Therefore, no power in the world can reject such a power which is indicative of personal life and which enables making inferences of habits and preferences.

One of the major findings of this thesis is that certain features of algorithms such as autonomous, opaque, decision-making and gate-keeping with capacities of learning, prioritizing, micro-targeting leads to ethical problems. These ethical problems were conceptualized as *invasion of privacy, discrimination, bias, automation, ossification, manipulation, asymmetry, appetite of consumption, data ownership, consumerism* and *commercialization* and they were dealt in greater detail within the chapter two.

For such ethical problems, again the importance of studying ethics of data was suggested as an answer. It argues that data ethics is responsive to discussions surrounding algorithmic culture which consists of data, algorithms and relevant practices. It is also concluded that data ethics as a field is inclusive of emerging problems in socio-technological assemblages which were determined as *hyper connected* and *networked* power relations, *concept of agency, knock-on effects, knowable outcomes, unstable nature of algorithms* and *the problem of many hands.* It is argued that data ethics is comprehensive enough to handle these problems. Thus, data ethics is found suitable, inclusive and constructive in framing and addressing ethical problems and offering solutions.

Ethics map the major contribution of this thesis presented in the second chapter revealed that its structure and framework enable us to conceptualize ethical problems, features of algorithms and types of algorithms. It is with the ethics map that it was possible to show that there exists no “single axis” between the three, allowing different focuses to interact (Floridi & Taddeo, 2016, p. 4). It is found that ethics map was diverse enough to handle different case studies empirically.

One important conclusion with regard to algorithms is that the study realized that there is a tendency to blame algorithms, leading them to be scapegoat for the emerging problems and attributing adjectives to algorithms such as discriminative, racist, anti-Semitic and etc. which actually belong human-beings. However, the thesis claims that algorithmic and computing systems should not be the scapegoat where people put blame of the unethical results of their technological conducts. Because it is understood that algorithms as scapegoat is an idea that reaches to nowhere. An algorithm cannot be racist or discriminative. It can produce biased results. Then, the question should be why algorithm produces biased result. Therefore, it is believed that the focus and center is on the wrong place in many studies.

It is concluded that algorithms can produce biased and unfair results, because there can be biases on the training data or in the data set: data collection and data selection process can be biased: the design of the system can be biased: technologists or developers' own prejudices can get baked into algorithms. Also, it is concluded that an algorithm is a logic to protect status quo, if data or design are biased or if developer transmits her/his biases into algorithm, then algorithm will further the bias. In this sense, it is found that algorithms and data are reflective of the society. The question is that can we develop technology which can take the best of human beings, not the worst sides of our society (Lee, 2016)? Is it really possible? If yes, where would this lead us -not only as human beings but also as social scientists working on such issues-?

Furthermore, there are 'many hands' in the algorithmic systems, contributing to development of technology. Thus, blaming an algorithm for ethical problems, when the reality should actually be a distributed morality, is considered as taking the easy way out of the problem without holding any responsibility. And, it is also considered as defaming and scandalizing of algorithms and technologies. And, maybe in this way, scientists who develop technology can start questioning the problem of how they study science without understanding the society itself, its problems and its Geist in the first place. Besides, the problem of developing technology for the society without knowing the society itself can come into prominence.

In respect to this, this study by questioning morality, intentionality, responsibility and accountability of machine agents argued whether or not they are accountable for their outputs. It is discussed that we can attribute *functional moral responsibility* (Dodig Crnkovic & Çürüklü, 2012) to machine agents. Because algorithmic agents have regulatory roles in technological systems acting as decision makers and gate keepers with some degree of autonomy, leading them to gain agency. For this reason, these agents are considered as functionally morally responsible. However, only on the condition that they are seen as parts of socio-technological assemblages where responsibility and accountability are discussed as *distributed* and *networked* morality between human and non-human agents. However, this study being aware of the economy politics of the companies concludes that institutions and individuals who develop technology should have a bigger slice from the responsibility and accountability discussion, and they should own the outcomes of negative impacts of their technology.

Moreover, the ethical perspective of this study suggested that no single ethical approach can be adopted, because ethical problems are diverse and there is not a standard for the problems. Therefore, there cannot be any ethical standard approach to adopt. Instead, it is suggested that ethics do not emerge out of a void, they cannot be implemented only via principles and guidelines, ethics cannot be inserted into technological systems by following dos and don’ts. Ethics requires cultural and social practice, individual and social responsibility in the form of morals and accountable decision-making, as much as it requires institutional codes of conduct, regulations, in-depth consideration for the outcomes of technology and reflections for the design and practice. It is concluded that only in this way ethics of algorithms can work for individuals, companies and governments.

This study offered regulatory responses for the ethical problems to show what could be our action for unethical practices of governments and companies and for the disparate impacts of algorithms. These regulatory responses were discussed as *accountability, transparency, notification* and *direct regulation of governments and institutions.* The stance of this study is that as much as we need governmental bodies, institutional control for the technological practices of individuals and companies, we need ethical understanding first. Ethical thinking needs to flourish and needs to be cultivated first to have ethical outcomes. By some literature, ethical responses were considered as soft responses. However, this study disagrees. Ethical response can stay as a soft response, if it only comes from the academia, without rising from the individuals and groups in the society. Because what brings the change is the society. If society demands ethical practices, then companies or governments will be forced to ethical behavior. It is thought that our studies are important to trigger ethical discussion within the society. However, we need to find ways to embed ethical thinking into society, if we want to live in ethical societies. But how can we sustain ethics in the society? In order to achieve this, it is believed that values of the society need to change. Values of individuals or groups of the society can change and ethics can be taught. And, we need change because each era brings new needs and those new needs inevitably require new perspectives and values. Then, the question is how will it be possible?

As a conclusion, there are five possible ways determined to achieve this goal. The first one is through *education*. Data literacy and new media literacy educations should be given which make members of the society aware of the problem, understand the importance of the problems, realize why ethics is necessary as a response, comprehend how problems can be tackled and what kinds of actions can be taken by citizens. Also, educations on (communication, work or data) ethics can be provided at schools as parts of curriculum and at workplaces as programs aiming to explain the problems of the society to people who develop technology. The second one can be achieved through the works of *NGOs.* Awareness for ethical problems can also be achieved by drawing attention to NGOs working on the problems of information societies. Effort of civil actors can be facilitated, supported and opportunities can be created to make their works visible. The third one is through *public service ads*. They can be effective in raising a question mark in minds or in informing publics. Online and offline world can be used as a space of publics service ads ranging from bus/metro stations, billboards, TV, radio to online platforms and social media. The forth one can be achieved by *companies.* Private companies which create the online services can create awareness by notification and with simplified and tangible expressions regarding privacy and decision-making processes. The fifth one is through *governmental support*. Governments can prepare reports covering the ethical issues, making sure that problems are visible and understandable, offering solutions and framing dis/advantages of the technologies. In sum, we need everything for ethics to cultivate in the society: codes of conducts, principles, external audit, disciplined commitment, enforcement, individual and social responsibility, accountability and efforts from all parts such as governments, companies, citizens, technologists and civil actors.

And, it is concluded that if there is not enough ethical discussion, then the social consensus will be formed in that direction. And, examples of unethical practices will be normalized and they will be stabilized.

The statement of the thesis does not have the purpose to be an episode of Black Mirror, but if we do not take an action for the way companies develop technology and how governments engage with data-driven algorithms, it is believed that people will be abused more, personal data will be commodified and human life, practice, habits and conduct will be exposed to commercialization more and more. This is simply because technology will continue to develop in a very fast pace: there will be more sensors that will communicate with each other which will bring more efficiency and which will infer more meaning from our lives: more and more parts of our lives will be digitalized and convergence will increase.

And, lastly the situation in Turkey with regards to data, algorithms and the Internet will be reviewed with examples. There are new opportunities, contributions and possibilities that the Internet and data-driven technologies have provided to us. However, there are also a variety of problems such as censorship, blockings, bans on the Internet usage etc. Also, the more institutions have become aware of data as an economic input of the information societies, the more data are commodified, sold and shared. Not only economic incentives, but also indicative nature of data made governmental bodies aware of the possibilities to make citizens see-through. The discussions are mainly centered on the protection of personal data, health data, data ownership, dataveillance and regulations. And, it is possible to say that ethical problems experienced in Turkey have three main branches: citizens being unconscious, reckless and unaware of the problems: governmental bodies regulating usage of the Internet and data for surveillance or economic incentives and companies trying to gain profit from the data. The main aim is not to discuss every situation, but to create a general understanding of the situation in Turkey with prominent examples:

-On bans, blockings, shutdowns and blackouts: Access to YouTube was blocked for two years (Bianet, 2010): Twitter was blocked in 2014 (Hürriyet Daily News, 2014): Vimeo was banned in 2014 (Bianet, 2014): 80.000 web sites were blocked in 2015 and only 5% of them were conducted with court decision, according to report of European Commission (Avrupa Komisyonu, 2015, p. 69): Dropbox, Google Drive, Microsoft OneDrive and Github was blocked in 2016 (Turkey Blocks, 2016a): Internet was shut down on southeast of Turkey for six days (Turkey Blocks, 2016b): Wikipedia has been blocked since April 29, 2017 (Phippen, 2017): VPN services which are used as a response to bans are also banned (Diken, 2018).

- On throttling: Social media platforms and the Internet throttling has become a new active tool for institutions to control communication and information flow. It has been realized that in many political/security contexts such as after terrorist attacks (Freedom House, 2017), coup attempt (Kırlıdoğ & Akgül, 2016), leaks on political corruptions, video release of execution of Turkish soldiers by ISIS (Turkey Blocks, 2016c), network traffic was controlled by Internet Service Providers (ISPs) by throttling the band-width. It is argued that this is a way of censorship. Furthermore, prime minister has accepted the slowdown of the Internet by saying that such measures may be taken for security reasons (Hürriyet Daily News, 2016).

-On commodification, commercialization and security of personal data: it is revealed that Social Security Institution sold citizens' health data for 65 thousand Turkish Liras back in 2013 (Nebil, 2018): data of students and teachers were stolen from the database of the Ministry of National Education (Radikal, 2015) and also personal data of the students were copied from the same database and sold to third parties by public officers (Milliyet, 2014): and lastly, personal data (name, surname, ID, father/mother name, full address etc.) of 50 million citizens of Republic of Turkey leaked online by Anonymous in 2016 (Tait, 2016).

- On Deep Packet Inspection (DPI): Usage of DPI means that governments and Internet Service Providers (ISPs) can read the contents of the data packets (Alternatif Bilişim Derneği, 2012). There are three basic usage area of DPI: network monitoring, targeted ads/behavioral targeting and legal or illegal surveillance/censorship by states (Kırlıdoğ & Fidaner, 2013, p. 2-3). As discussed by Alternatif Bilişim Derneği (2012), Information and Communication Technologies Authority had DPI produced by a company called C2Tech (C2Tech, n.d.).

Thus, it is seen that there have been continuous bans, blockings, shutdowns and blackouts over the last ten years in Turkey. Measures taken such as usage of VPN are mainly temporary and do not solve the problem with regard to citizens' right to communication, right to Internet access and right to privacy. It is believed that we as citizens and users need to have a more holistic and integrated approach for our online rights. Security of data, personal data and even health data is weak and not protected enough and they are even commodified by the public officers. It is believed that we need to find ways of claiming data ownership and protection of personal data. Throttling, deep packet inspection or other ways of violations are considered as illegal in terms of right to privacy and confidentiality. In this sense, ISPs and government are breaching this right and making the Internet less secure. Apart from that, it is also possible to talk about a section of the society which do not care about breaches, which are not aware of the value of data, which think government have the right to make citizens transparent. Thus, violations become easier in a society, if there is not enough counterforce. Therefore, it is important to support works of civil actors working through educations, projects and trainings to discuss problems, to communicate importance of the issues and to show ways of demanding our online and offline rights. In this regard, this research would like to end the discussion by pointing out to NGOs working on the field (including but not limited to): Data Literacy Association, Alternative Informatics Association, Turkey Blocks, İnternet Teknolojileri Derneği, Toplumsal Bilgi ve İletişim Derneği and Şeffaflık Derneği.

Suggestions for the future research which are beyond the scope and limitations of this thesis are listed below:

- A research on algorithmic culture can also focus on good data practices which make use of capacities of algorithms. For instance, the research can inspect algorithms which are used to support public interest and to develop new possibilities in healthcare, economy, education, regulation and etc.

- This thesis study focused on subjective and complex algorithms working on OSPs. However, a further research can focus different areas such as smart homes, smart cities and smart municipalities which is believed to be more important in the coming years, as more sensors will be communicating with each other in the future.

- In accordance with the demands of the NGOs, a study can be conducted with NGOs which work on open data, data journalism, data literacy and data visualization in Turkey in order to increase awareness towards data and components of our modern digital information societies.

- A study can focus on behavioral targeting practices of big companies that deploy proprietary algorithms to profile and track users and to targets ads, products and goods for specific individuals. Their economy politics, business structure and ecology can be studied to understand how they make use of data.
- Data literacy can be studied by providing educations at schools to make users gain agency and to explain how information societies work. It can also test if awareness towards data and algorithms will increase responsible behavior.
- An analysis of how governments and companies make use of data and algorithms during social movements to track, profile and target people which aims to challenge public opposition and critical thinking can be studied.
- An ethical monitoring study can be conducted to monitor and to report the violations conducted by the parties (governments, companies or individuals) concerning the personal data.

REFERENCES

Acquisti, A. (2014). The economics and behavioral economics of privacy. In J. Lane, V. Stodden, S. Bender & H. Nissenbaum (Ed.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 76-95). New York: Cambridge University Press.

Adblock Plus. (n.d.). *Adblock plus features.* Retrieved April 29, 2018 from https://adblockplus.org/en/features#tracking

Albert. (2016, February 28). Is there a difference between open data and public data? Message posted to https://opendata.stackexchange.com/questions/7143/is-there-a-difference-between-open-data-and-public-data

Allen-Castellitto, A. (1999). Coercing privacy. *William and Mary Law Review*, 40, 723-757.

Allen, C., Wallach, W. & Smit, I. (2006). Why machine ethics? *IEEE Intelligent Systems*, *21*(4), 12-17. DOI: 10.1109/MIS.2006.83

Al-Sharif, M. (2018, September 16). The dangers of digital activism. *The New York Times.* Retrieved from https://www.nytimes.com/2018/09/16/opinion/politics/the-dangers-of-digital-activism.html

Alstyne, M., & Brynjolfsson, E. (1997). Electronic Communities: Global Village or CyberBalkans. In *Proceedings of the 17th International Conference on Information Systems.* Retrieved from Massachusetts Institute of Technology http://web.mit.edu/marshall/www/papers/CyberBalkans.pdf

Alternatif Bilişim Derneği. (2012). *Türkiye'de internetin durumu.* Retrieved from https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/alternatif_bilisim_internet_raporu.pdf

Ananny, M. (2011, April 14). The curious connection between apps for gay men and sex offenders. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340/

Ananny, M. (2016). Toward an ethics of algorithms: Convening, observation, probability, and timeliness. *Science, Technology, & Human Values*, 41(1), 93-117. DOI: 10.1177/0162243915606523

Ananny, M., & Crawford, K. (2016). Seeing without knowing. Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 1-17. DOI: 10.1177/1461444816676645

Anderson, M. & Anderson, S.L. (2007). Machine ethics: Creating an ethical intelligent agent. *AI Magazine, 28*(4), 15-26.

Anderson, S. L. (1995). Being morally responsible for an action versus acting responsibly or irresponsibly. *Journal of Philosophical Research, 20,* 453-462.

Anderson, S. (2013, December 6). *Google toolbar Pagerank update history.* Retrieved April 29, 2018, from Hobo UK SEO Services https://www.hobo-web.co.uk/google-pr-update/

Anderson, S. (2018, March 28). *SEO tutorial for beginners in 2018.* Retrieved April 29, 2018, from Hobo UK SEO Services https://www.hobo-web.co.uk/seo-tutorial/

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, 16(1), 19-36. DOI: 10.1177/1527476414541552.

AOIR. (2017, January 11). *AOIR ethics graphic 2016.* Retrieved from https://aoir.org/wp-content/uploads/2017/01/aoir_ethics_graphic_2016.pdf

Aristotle. (1998). *The nicomachean ethics.* (F.H. Peters & M. Ostwald, Trans.). Oxford: Oxford University Press.

Arthur, C. (2014, March 27). Google Flu Trends is no longer good at predicting flu, scientists find. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2014/mar/27/google-flu-trends-predicting-flu

Avital, M., Sawyer, S., Kraemer, K., Sambamurthy, V., Lyytinen, K., & Iacono, C.S. (2007). Data rich and data poor scholarship: Where does IS research stand? *ICIS 2007 Proceedings, 101*. Retrieved from https://aisel.aisnet.org/icis2007/101

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671-732.

Avrupa Komisyonu. (2015). *Komisyon çalışma dökümanı 2015 yılı Türkiye raporu.* Retrieved from https://www.ab.gov.tr/files/000files/2015/11/2015_turkiye_raporu.pdf

Battelle, J. (2005). *The search: How Google and its rivals rewrote the rules of business and transformed our culture.* New York: Penguin.

Bauman, Z. (2007). *Consuming Life.* Cambridge: Polity Press.

Beck, L.W. (1997). Translator's introduction. In *Foundations of the metaphysics of morals* (2nd ed.). Upper Saddle River, NJ: Library of Liberal Arts/Prentice Hall.

Ben-Porat, O., & Tennenholtz, M. (2018). Competing prediction algorithms. *arXiv preprint arXiv: 1806.01703,* 1-17.

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society,* 11(6), 985-1002. DOI: 10.1177/1461444809336551

Betters, E. (2014, April 26). *What does Facebook own? Here's the companies it has acquired and the reasons why*. Retrieved April 27, 2018, from Pocket-lint https://www.pocket-lint.com/apps/news/facebook/128617-what-does-facebook-own-here-s-the-companies-it-has-acquired-and-the-reasons-why

Bianet. (2010, October 29). YouTube yasağı kalkıyor mu yoksa? *Bianet*. Retrieved from http://bianet.org/bianet/ifade-ozgurlugu/125737-youtube-yasagi-kalkiyor-mu-yoksa

Bianet. (2014, January 10). Vimeo banned in Turkey. *Bianet*. Retrieved from https://m.bianet.org/english/freedom-of-expression/152728-vimeo-banned-in-turkey

Binark, M. & Altıntaş, M. (2016). Veri ikizlerimizin farkında mıyız? Dijital gözetimin çeşitli boyutlarına karşı farkındalık. B, Özçetin, C., Sözeri, İ., Sayımer, İ., İnceoğlu, P., Öğün Emre, T., Çomu (Ed.). *Yeni Medya Çalışmaları II. Ulusal Kongre* (s. 315-334) Ankara: Alternatif Bilişim Derneği.

Binark, M. (2017). Algoritmaların yarattığı yankı odalarında siyasal katılımın olanak/sızlı/ğı. *Varlık,* 1317, 19-23.

Botsman, R. (2017, October 21). Big data meets big brother as China moves to rate its citizens. *Wired.* Retrieved from https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662-679. DOI: 10.1080/1369118X.2012.678878

Bozdağ, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and Information Technology*, 15(3), 209-227. DOI: 10.1007/s10676-013-9321-6.

Bozdağ, E. (2015). *Bursting the filter bubble: Democracy, design and ethics.* (Doctoral dissertation). Retrieved from TU Delft Repositories. (DOI: DOI: 10.4233/uuid:87bde0a2-c391-4c77-8457-97cba93abf45)

Brevoort, K. P., Grimm, P., & Kambara, M. (2015, May). Data point: Credit invisibles. Retrieved from https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf

Bucher, T. (2012). Want to be on the top? Algorithmic Power and the threat of invisibility on Facebook. *New Media & Society*, 14(7), 1164-1180. DOI: 10.1117/1461444812440159

Bulut. E. (2016). Beğeniyorum öyleyse varım: Sosyal medyada içerik üretimi, yabancılaşma ve sömürü. *İktisat ve Toplum, 71*, 20-28.

Bulut. E. (2018). Interview with Safiya U. Noble: Algorithms of oppression, Gender and Race. *Moment Journal*, *5*(2): 294-301. Retrieved from http://www.momentdergi.org/index.php/momentdergi/article/view/349/602

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society,* 3(1): 1-12. DOI: 10.1177/2053951715622512.

Bynum, T. (2015). Computer and information ethics. In E.N. Zalta (Ed.), *The Sandford encyclopedia of philosophy* (Winter 2015 Ed.). Retrieved from https://plato.stanford.edu/archives/win2015/entries/ethics-computer/

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Calhoun, C. J. (Eds.). (2002). *Dictionary of the social sciences.* New York: Oxford University Press.

Campolo, A., Sanfilippo, M., Whittaker, M., & Crawford, K. (2017). *AI Now Report 2017.* Retrieved from https://ainowinstitute.org/AI_Now_2017_Report.pdf

Carah, N. (2017). Algorithmic brands: A decade of brand experiments with mobile and social media. *New Media & Society,* 19(3), 384-400.

Cardona, B. (2008). 'Healthy ageing' policies and anti-ageing ideologies and practices: On the exercise of responsibility. *Medicine, Health Care and Philosophy*, *11*(4), 475-483.

Castelluccia, C. (2012). Behavioural tracking on the Internet: A technical perspective. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Ed.), *European data protection: In good health?* (pp. 21-33). Dordrecht: Springer.

Chang, A. (2018, May 2). The Facebook and Cambridge Analytica scandal, explained with a simple diagram. *Vox.* Retrieved from https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society*, 28(6), 164-181.

Clarke, R. (1998). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498-512

Clarke, R. (2016). Induction to dataveillance and information privacy, and definitions of terms. Retrieved May 1, 2018, from: http://www.rogerclarke.com/DV/Intro.html#Mis

Clarke, R. (2018). Clarke's dataveillance and information privacy home-page. Retrieved May 1, 2018, from http://www.rogerclarke.com/DV/#SurvD

Clarke, R., & Greenleaf, G. (2018). Dataveillance regulation: A research framework: Retrieved May 1, 2018, from http://www.rogerclarke.com/DV/DVR.html

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., & Swire, P. P. (2013, December 19). Protecting citizens, and their privacy. *The New York Times*. Retrieved from https://www.nytimes.com/2013/12/20/opinion/protecting-citizens-and-their-privacy.html

Coeckelbergh, M. (2010). Moral appearances: Emotions, robots, and human morality. *Ethics and Information Technology, 12*(3), 235-241.

Cohn, J. (2016). My TiVo thinks I'm gay: Algorithmic culture and its discontents. *Televison & New Media,* 17(8), 675-690. DOI: 10.1177/1527476416644978.

Computer Ethics Institute. (2011). *The ten commandments of computer ethics.* Retrieved January 15, 2019 from http://cpsr.org/issues/ethics/cei/

Cortland, M. (2017, February 1). *The state of the blocked web: 2017 Global Adblock Report.* Retrieved from https://pagefair.com/blog/2017/adblockreport/

Costanza-Chock, S. (2018). *So you want to disrupt the matrix of domination? Towards a design justice approach to data interventions* [PowerPoint slides]. Retrieved from https://docs.google.com/presentation/d/1nZSaBdk_RGkYQsjtO83LaRs_AjDBQ5tKAxcrI30FQ7s/edit#slide=id.p

Couldry, N. (2012) *Media, Society, World.* Cambridge: Polity Press.

Crawford, K. (2013, April 1). The hidden biases in big data. *Harvard Business Review*. Retrieved from https://hbr.org/2013/04/the-hidden-biases-in-big-data

Crawford, K. (2016). Can an algorithm be agonistic? Ten scenes from life in calculated publics. *Science, Technology, & Human Values, 41*(1), 77-92. DOI: 10.1177/0162243915589635

C2Tech. (n.d.). *Deep packet inspection.* Retrieved from https://www.ctech.com.tr/technology/derin-paket-incelemesi/

Custers, B. (2013). Data dilemmas in the information society: Introduction and overview. In B. Custers, B. Schermer, T. Calders & T. Zarsky (Ed.), *Discrimination and privacy in the information society* (pp. 3-26). Springer-Verlag Berlin Heildelberg

Damasio, A. R. (1994). *Descartes' Error: Emotion, reason, and the human brain.* New York: Avon.

de Vries, K. (2010). Identity, profiling algorithms and a world of ambient intelligence. *Ethics and Information Technology, 12*(1), 71-85.

Dewey, J. (1891). Moral theory and practice. *International Journal of Ethics, 1*(2), 186-203. Retrieved from http://www.jstor.org/stable/2375407

Diakopoulos, N. (2015). Algorithmic accountability: Journalistic investigation of computational power structures. *Digital Journalism*, 3(3), 398-415.

Dietrich, E. (2006). *After the humans are gone.* Keynote address presented at the 2006 North American Computing and Philosophy Conference, RPI, Troy, NY.

Diken. (2018, March 16). Bu da oldu: Erişim engelini aşan VPN hizmetlerine de erişim engeli getirildi. *Diken.* Retrieved from http://www.diken.com.tr/bu-da-oldu-erisim-engelini-asan-vpn-hizmetlerine-de-erisim-engeli-getirildi/

Dodge, M., and Kitchin, R. (2009). Software, objects, and home. *Environment and Planning A*, 41(6), 1344-1365.

Dodig-Crnkovic, G. (2006). *Professional ethics in computing and intelligent systems.* Proceedings of the Ninth Scandinavian Conference on Artificial Intelligence (SCAI 2006), Espoo, Finland.

Dodig-Crnkovic, G., & Çürüklü, B. (2012). Robots: Ethical by design. *Ethics and Information Technology, 14*(1), 61-71. DOI: 10.1007/s10676-011-9278-2

DoubleClick. (n.d.-a). *Digital advertising solutions.* Retrieved 30 April, 2018, from https://www.doubleclickbygoogle.com/

DoubleClick. (n.d.-b). *Ad sales management for publishers.* Retrieved April 30, 2018, from https://www.doubleclickbygoogle.com/solutions/revenue-management/dfp/?_ga=2.94226589.1602275084.1514202839-800107452.1514202839

Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. *Big Data & Society,* 3(2), 1-11. DOI: 10.1177/2053951716665128

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times*. Retrieved from https://mobile.nytimes.com/2012/02/19/magazine/shopping-habits.html?smid=fb-share&referer=http://m.facebook.com

Eagle. N., & Pentland, A. S. (2006). Reality mining: Sensing complex social systems. *Personal and Ubiquitous Computing*, 10(4), 255-268.

Elmer, G. (2004). *Profiling Machines*. Cambridge, MA: MIT Press

ESOMAR. (2009). ESOMAR World Research Codes & Guideliness Passive Data Collection, Observation and Recording. Retrieved April 26, 2018, from esomar.orghttps://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Codes-and-Guidelines_Passive_Data_Collection-Observation-and-Recording.pdf

Eubanks, V., Angwin, J., & Nelson, A. (2018, January 22). *Databite No 106: Virginia Eubanks* [Video file]. Retrieved May 1, 2018, from https://www.youtube.com/watch?time_continue=3150&v=v01_--OiHGo

European Parliament & Council of EU. (1995, October 24). *Directive 95/46/EC of the European Parliament and of the Council*. Retrieved from http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

Federal Trade Commission. (2009, February 12). *FTC staff revises online behavioral advertising principles*. Retrieved April 30, 2018, from https://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles

Flood, A. (2016, November 15). ‘Post-truth’ named word of the year by Oxford Dictionaries. *The Guardian*. Retrieved from https://www.theguardian.com/books/2016/nov/15/post-truth-named-word-of-the-year-by-oxford-dictionaries

Floridi, L. (2013). Distributed morality in an information society. *Science and Engineering Ethics*, *19*(3), 727-743. DOI: 10.1007/s11948-012-9413-4

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*(1), p. 1-3. DOI: 10.1007/s13347-014-0157-8

Floridi, L., & Sanders, J.W. (2004). On the morality of artificial agents. *Minds and Machines*, *14*(3), 349-379.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 1-4.http://doi.org/10.1098/rsta.2016.0360

Freedom House. (2017). *Freedom on the net 2017: Turkey*. Retrieved from https://freedomhouse.org/report/freedom-net/2017/turkey

Fried, C. (1968). Privacy: A moral analysis. *Yale Law Journal,* 77(1), 475-493.

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems, 14*(3), 330-347.

Friedman, B., Kahn, P. H., & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang & D. Galletta (Ed.), *Human-computer interaction in management information systems: Foundations* (pp. 348-372). London, UK: M.E. Sharpe.

Froomkin, A. M. (2000). The death of privacy? *Stanford Law Review,* 52, 1461-1543.

Fuchs, C. (2011). *A contribution to the critique of the political economy of Google.* Retrieved April 26, 2018, from http://fuchs.uti.at/wp-content/uploads/Google_FastCapitalism.pdf

Fussell, S. (2018, July 2). Boston police used Twitter and Facebook to surveil protestors using the #MuslimLivesMatter hashtag. *Gizmodo.* Retrieved from https://gizmodo.com/boston-police-used-twitter-and-facebook-surveil-protest-1822814877

Galloway, A.R. (2006). *Gaming: Essays on Algorithmic Culture.* Minneapolis, MN: University of Minnesota Press.

Garett, S. (2015, December 11). 2016 year in preview: Ad targeting toes the creepy line. *Digiday UK.* Retrieved from https://digiday.com/marketing/2016yearinpreview-targeting-ads-get-lot-creepier/

Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User profiles for personalized information access. In P. Brusilovsky, A. Kobsa & W. Nejdl (Eds.), *The adaptive web: Methods and strategies of web personalization* (pp. 54-89). Berlin Heildelberg: Springer.

Gavison, R. (1980). Privacy and the limits of the law. *Yale Law Journal,* 89, 421-427.

Geofeedia. (2017). *Location-based analytics platform.* Retrieved from https://geofeedia.com/

Gillespie, T. (2010). The politics of ‘platforms’. *New Media & Society,* 12(3), 347-364.

Gillespie, T. (2012). *Can an algorithm be wrong?* Retrieved April 25, 2018, from Limn: Crowds and Clouds: https://limn.it/articles/can-an-algorithm-be-wrong/

Gillespie, T. (2014). The relevance of algorithms. In Gillespie T., Boczkowski P., & Foot K., (Ed.) *Media Technologies: Essays on Communication, Materiality, and Society* (pp. 167- 194). Cambridge, MA: The MIT Press.

Gillespie, T. (2016). Algorithm. In B. Peters (Ed.), *Digital Keywords: A vocabulary of information society & culture* (pp. 18-30). Princeton, NJ: Princeton University Press.

Goel, V. (2014, June 29). Facebook tinkers with users' emotions in newsfeed experiment, stirring outcry. *The New York Times.* Retrieved from https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html

Goffey, A. (2008). Algorithm. In Fuller, M. (Ed.) *Software Studies: A Lexicon* (pp. 15-20). Cambridge, MA: MIT Press.

Goldman, E. (2006). Search engine bias and the demise of search engine utopianism. *Yale Journal of Law & Technology, 8*, 188-200.

Goldschlager, L., & Lister, A. (1988). *Computer Science: A Modern Introduction.* (2nd ed.). Hemel Hempstead: Prentice- Hall.

Google. (n.d.). In *Oxford Dictionaries online.* Retrieved from https://en.oxforddictionaries.com/definition/google

Google. (n.d.-a). *Welcome to the Google privacy policy.* Retrieved December 27, 2017, from Google Privacy & Terms https://policies.google.com/privacy?hl=en

Google. (n.d.-b). *Advertising.* Retrieved December 27, 2017, from Google Privacy & Terms https://policies.google.com/technologies/ads?hl=en

Google. (n.d.-c). *Targeting your ads.* Retrieved December 27, 2017, from support.google https://support.google.com/adwords/answer/1704368?hl=en

Google. (n.d.-d). *Ads you can count on*. Retrieved December 27, 2017, from Google AdSense https://www.google.com/adsense/start/#/?modal_active=none

Google. (n.d.-e). *Manage Google voice & audio activity.* Retrieved December 27, 2017, from support.google https://support.google.com/websearch/answer/6030020?p=account_voice_audio&hl=en&authuser=0&visit_id=1-636506054156391446-566086102&rd=1

Google. (n.d.-f). *Costumer journey & user behavior analysis.* Retrieved December 27, 2017, from Google Analytics Solutions https://www.google.com/intl/en_uk/analytics/analytics/capabilities/

Google. (n.d.-g). *About remarketing.* Retrieved December 27, 2017, from support.google https://support.google.com/adwords/answer/2453998?hl=en

Granka, L.A. (2010). The politics of search: A decade retrospective. *The Information Society*, *26*(5), 364-374. DOI: 10.1080/01972243.2010.511560.

Greene, D. (2017, June 23). *As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align.* Retrieved 27 April, 2018, from blog.google: https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

Greenwood, D., Stopczynski, A., Sweatt, B., Hardjono, T., & Pentland, A. (2014). The new deal on data: A framework for institutional controls. In In J. Lane, V. Stodden, S. Bender & H. Nissenbaum (Ed.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 192-210). New York: Cambridge University Press.

Griffin, A. (2016, June 1). Google voice search records and keeps conversations people have around their phones – but the files can be deleted. *Independent.* Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-voice-search-records-stores-conversation-people-have-around-their-phones-but-files-can-be-a7059376.html

Guha, S., Cheng, B., & Francis, P. (2010, November). Challenges in measuring online advertising systems. In *proceedings of the 10th ACM SIGCOMM conference on Internet measurement* (pp. 81-87). ACM. Retrieved from: https://dl.acm.org/citation.cfm?id=1879152

Hallinan, B., & Striphas, T. (2016). Recommended for you: The Netflix prize and the production of algorithmic culture. *New Media & Society*, 18(1), 117-137. DOI: 101177/1461444814538646

Hannak, A., Sapiezynski, P., Kakhki, M., Krisnamurthy, B., Lazer, D., Mislove, A., & Wilson, C. (2013 May). Measuring personalization of web search. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 527-538). ACM. Retrieved from https://dl.acm.org/citation.cfm?id=2488435

Hearn, A. (2010). Structuring feeling: Web 2.0, online ranking and rating, and the digital 'reputation' economy. *ephemera: theory & politics in organization, 10(3/4), 421-438.*

Heath, A. (2017, January 18). Mark Zuckerberg explains Facebook's secrets for acquiring companies. *Business Insider*. Retrieved from http://www.businessinsider.com/mark-zuckerberg-explains-facebooks-acquisition-strategy-2017-1

Hern, A. (2017, June 20). Google will stop scanning content of personal emails. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/jun/26/google-will-stop-scanning-content-of-personal-emails

Hern, A. (2018, January 12). Google's solution to accidental algorithmic racism: ban gorillas. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people

Hildebrandt, M. (2006). Profiling: From data to knowledge. *DuD. Datenschutz und dtensicherheit, 30*(9), 548-552.

Hildebrandt, M., & Koops, B-J. (2010). The challenges of ambient law and legal protection in the profiling era. *The Modern Law Review, 73*(3), 428-460.

Himo, J., & Carron, C. (2016, November 4). *IP addresses as personal information: The Canadian and EU positions contrasted.* Retrieved April 30, 2018, from Data Protection Report: https://www.dataprotectionreport.com/2016/11/ip-addresses-as-personal-information-the-canadian-and-eu-positions-contrasted/

Honan, M. (2014, August 8). I liked everything I saw on Facebook for two days. Here is what it did to me. *Wired.* Retrieved from https://www.wired.com/2014/08/i-liked-everything-i-saw-on-facebook-for-two-days-heres-what-it-did-to-me/

Horling, B., & Kulick, M. (2009, December 4). *Personalized search for everyone.* Retrieved April 25, 2018, from Google Official Blog: https://googleblog.blogspot.com.tr/2009/12/personalized-search-for-everyone.html

Hursthouse, R. (1999). *On virtue ethics.* Oxford: Oxford University Press.

Hürriyet Daily News. (2014, March 20). Turkey blocks Twitter, after Erdoğan vowed 'eradication'. *Hürriyet Daily News.* Retrieved from http://www.hurriyetdailynews.com/turkey-blocks-twitter-after-erdogan-vowed-eradication-63884

Hürriyet Daily News. (2016, November 4). Slowdown in access to social media in Turkey a 'security measure,' says PM. *Hürriyet Daily News.* Retrieved from http://www.hurriyetdailynews.com/slowdown-in-access-to-social-media-in-turkey-a-security-measure-says-pm-105744

Isidore, C. (2015, June 10). RadioShack sale protects most consumer data. *CNN Money.* Retrieved from https://money.cnn.com/2015/06/10/news/companies/radioshack-customer-data-sale/index.html

Jagadish, H.V. (2016). Data Science Ethics. *Edx Online Course.* Retrieved from: https://courses.edx.org/courses/course-v1:MichiganX+DS101x+3T2016/course/

Jane Doe v Netflix. (2009, December 17). Original complaint (United States District Court for the Northern District of California). Retrieved from https://www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf

Johnson, J.A. (2006). Technology and pragmatism: From value neutrality to value critically. *SSRN Electronic Journal.* DOI: 10.2139/ssrn.2154654

Just, N., & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic selection on the Internet. *Media, Culture & Society*, 39(2), 238-258. DOI: 10.1177/0163443716643157.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, 50(4), 1193-1294.

Kelley, R. (2017, January 19). Machine learning explained: Algorithms are your friend. [web log comment]. Retrieved from https://blog.dataiku.com/machine-learning-explained-algorithms-are-your-friend

Kennedy, H. (2016). *Post, mine, repeat: Social media data mining.* London: Palgrave Macmillian.

Kırlıdoğ, M., & Fidaner, I. B. (2013). *Derin veri analizi: İnternet'teki temel gözetim aracı*. Akademik Bilişim Konferansı 2013, Antalya. Retrieved from https://ab.org.tr/ab13/bildiri/327.pdf

Kırlıdoğ, M., & Akgül, M. (2016, September 14). The internet and the recent coup attempt in Turkey. *Internet Policy Review.* Retrieved from https://policyreview.info/articles/news/internet-and-recent-coup-attempt-turkey/423

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. London: Sage.

Kopf, D. (2018, September 5). This is how computers "predict the future". *Quartz.* Retrieved from https://qz.com/1261817/predictive-algorithms-are-not-all-that-complicated/

Kowalski, R. (1979). Algorithm = logic + control. *Communications of the ACM*, *22*(7): 424 - 436.

Kraemer, U. A. F., Overveld, van, C. W. A. M., & Peterson, M. B. (2011). Is there an ethics of algorithms? *Ethics and Information Technology, 13*(3), 251-260. DOI: DOI: 10.1007/s10676-010-9233-7

Ladikas, M., Chaturvedi, S., Zhao, Y., & Stemerding, D. (2015). Introduction: Embedding ethics in science and technology policy – a global perspective. In M. Ladikas, S. Chaturvedi, Y. Zhao & D. Stemerding (Ed.), *Science and technology governance and ethics* (pp. 1-8). Cham: Springer.

Lambert, E. (2016, June 16). *Are IP addresses personal information.* Retrieved April 30, 2018, from Linkedin https://www.linkedin.com/pulse/ip-mac-addresses-personal-information-eric-lambert/

Laserfiche. (n.d.). *RadioShack bankruptcy asks: Who owns your data?* Retrieved from https://www.laserfiche.com/ecmblog/radioshack-bankruptcy-asks-who-owns-your-data/

Lash, S. (2007). Power after hegemony: Cultural studies in mutation. *Theory, Culture & Society*, 24(3), 55-78.

Lee, P. (2016, March 25). Learning from Tay's introduction. [web log comment]. Retrieved from https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/

Lewis, A. (2010, August 26). User-driven content. Retrieved May 2, 2018, from MetaFilter https://www.metafilter.com/95152/Userdriven-discontent#3256046

Lin, P., Bekey, G., & Abney, K. (2008, December 20). *Autonomous military robotics: Risk, ethics, and design.* Retrieved from http://ethics.calpoly.edu/ONR_report.pdf

Lowrie, I. (2018). Algorithms and automation: An introduction. *Cultural Anthropology, 33*(3), 349-359. https://doi.org/10.14506/ca33.3.01

Lyon, D. (2007). *Surveillance studies: An overview.* Cambridge: Polity Press.

Mackenzie, A. (2015). The production of prediction: What does machine learning want? *European Journal of Cultural Studies, 18*(4-5), 429-445. DOI: 10.1177/1367549415577384

Mager, A. (2012). Algorithmic ideology: How capitalist society shapes search engines. *Information, Communication & Society*, 15(5), 769-787.

Mahdawi, A. (2013, February 5). Can Googling be racist? *The Guardian.* Retrieved from https://www.theguardian.com/commentisfree/2013/feb/05/can-googling-be-racist

Marketing Türkiye. (2016, January 22). *Yemek Sepeti, "Büyük veri" kullanımı ile 4.5 milyon TL değer kazandı.* Retrieved 30 April, 2018, from https://www.marketingturkiye.com.tr/haberler/yemek-sepeti-buyuk-veri-kullanimi-ile-45-milyon-tl-deger-kazandi/

Markham, A.N. (2016, May 18). OKCupid data release fiasco: It's time to rethink ethics education. [web log comment]. Retrieved from https://points.datasociety.net/okcupid-data-release-fiasco-ba0388348cd

Markham, A. N. (2018). Afterword: Ethics as impact-moving from error-avoidance and concept-driven models to a future-oriented approach. *Social Media + Society*, *4*(3), 1-11. DOI: 10.1177/2056305118784504

Matthees, R. (2017, August 6). *How to track AdBlock users in Google Analytics even they block Javascript / Cookies.* Retrieved April 29, 2018 from https://www.robert-matthees.de/ecommerce/adblock-google-analytics/

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, *6* (3), 175-183.

McMullan, T. (2015, July 23). What does the panopticon mean in the age of digital surveillance? *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

McPherson, M., Smith-Lovin, L., & Cook, J.M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, 27(1), 415-444.

Merrill, J.C. (2011). Theoretical foundations for media ethics. In A.D. Gordon, J.M. Kittross & J.C.C. Merrill (Ed.), *Controversies in media ethics* (3rd ed., pp. 3- 32). New York: Routledge

Metoyer-Duran, C. (1993). Information gatekeepers. *Annual Review of Information Science and Technology (ARIST)*, 28, 111-150.

Meyer, R. (2018, March 20). The Cambridge Analytica scandal, in three paragraphs. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

Miglo, A. (2016). *Capital structure in the modern world.* Retrieved from https://link.springer.com/book/10.1007%2F978-3-319-30713-8

Miller, K., & Taddeo, M. (Eds.). (2017). *The ethics of information technologies. Library of essays on the ethics of emerging technologies.* New York, NY: Russell Sage Foundation.

Milliyet. (2014, October 6). Öğrenci bilgileri kopyalanıp satıldı. *Milliyet.* Retrieved from http://www.milliyet.com.tr/ogrenci-bilgileri-kopyalanip-gundem-1951022/

MinuteVideos. (2016, December 28). *Filter bubbles and echo chambers* [Video file]. Retrieved from https://www.youtube.com/watch?v=Zk1o2BpC79g

Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2): 1-21.

Mogan, E. (2014, August 14). I quit liking things on Facebook for two weeks: Here's how it changed my view of humanity. [web log comment]. Retrieved from https://medium.com/swlh/i-quit-liking-things-on-facebook-for-two-weeks-heres-how-it-changed-my-view-of-humanity-29b5102abace

Moor, J. (2006). The nature, importance, and difficulty of Machine Ethics. *IEEE Intelligent Systems, 21*(4), 18-21.

Morrison, K. (2014, April 30). *The NYPD will use Twitter to predict street crime.* Retrieved May 1, 2018, from Adweek: http://www.adweek.com/digital/nypd-twitter-predict-crime/

Mosseri, A. (2018, January). *Bringing people closer.* Retrieved April 26, 2018 from Facebook Newsroom https://newsroom.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/amp/?__twitter_impression=true

Munoz, C., Smith, M., & Patil, D. J. (2016). Big data: A report on algorithmic systems, opportunity, and civil rights. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

Naik, G., & Bhide, S. S. (2014). Will the future of knowledge work automation transform personalized medicine? *Applied & Translational Genomics, 3*(3), 50-53. https://doi.org/10.1016/j.atg.2014.05.003

Narayanan, A., & Shmatikov, V. (2006-2008). How to break anonymity of the Netflix Prize dataset. Retrieved May 1, 2018 from arXiv.org https://arxiv.org/abs/cs/0610105

Nebil, F. S. (2018, February 18). Danıştay'ın 'satılamaz' dediği sağlık verilerinin SGK tarafından 65 bin liraya satıldığı onaylandı. *T24.* Retrieved from https://t24.com.tr/yazarlar/fusun-sarp-nebil/danistayin-satilamaz-dedigi-saglik-verilerinin-sgk-tarafindan-65-bin-liraya-satildigi-onaylandi,19165

Netflix. (2018). *Netflix Prize.* Retrieved May 1, 2018, from https://www.netflixprize.com/

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datafication'. *The Journal of Strategic Information Systems*, 24(1), 3-14.

Neyland, D. (2016). Bearing account-able witness to ethical algorithmic system. *Science, Technology & Human Values,* 41(1), 50-76. DOI: 10.1177/0162243915598056

Nissenbaum, H. (1994). Computing and accountability. *Communications of the ACM*, *37*(1), 73-80.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* California: Stanford University Press.

Noble, S. [UCIBrenICS]. (2017, December 17). *Algorithms of oppression* [Video file]. Retrieved from https://www.youtube.com/watch?v=oqelqdDIDSs&feature=youtu.be

Normative ethics. (n.d.). In *Encyclopaedia Britannica online*. Retrieved from https://www.britannica.com/topic/normative-ethics

O'Neil, C. (2014, March 7). *An attempt to FOIL request the source code of the value-added model*. Retrieved from https://mathbabe.org/2014/03/07/an-attempt-to-foil-request-the-source-code-of-the-value-added-model/

O'Neil, C. (2016, September 1). How algorithms rule our working lives. *The Guardian.* Retrieved from https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives

Open Data Handbook. (n.d.). *What is open data?* Retrieved from http://opendatahandbook.org/guide/en/what-is-open-data/

O'Reilly, T. (2013). Open data and algorithmic regulation. In B. Goldstein & L. Dyson (Ed.), *Beyond transparency: Open data and the future of civic innovation* (pp. 289-300). San Francisco, CA: Code for America Press.

Page, V. (2015, May 18). *Top companies owned by Facebook (FB).* Retrieved April 26, 2018, from Investopedia: https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

Pariser, E. (2011a). *The filter Bubble: What the Internet is hiding from you.* UK: Penguin.

Pariser, E. (2011b). *Beware online "filter bubbles"* [Video file]. Retrieved from https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles

Pasquale, F. (2011). Restoring transparency to automated authority. *Journal of Telecommunication & High Technology Law*, 9, 235-254.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Cambridge: Harvard University Press.

Pasquinelli, M. (2009). Google's PageRank algorithm: A diagram of the cognitive capitalism and the rentier of the common intellect. In K. Becker & F. Stalder (ed.), *Deep search: The politics of search beyond Google.* London: Transaction Publishers. Retrieved from https://www.academia.edu/1992027/Googles_PageRank_Algorithm_A_diagram_of_Cognitive_Capitalism_and_the_Rentier_of_the_Common_Intellect

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The role of crime forecasting in law enforcement operations.* RAND Corporations.

Phippen, J. W. (2017, April 29). Why Turkey blocked access to Wikipedia. *The Atlantic.* Retrieved from https://www.theatlantic.com/news/archive/2017/04/turkey-blocks-wikipedia/524859/

Post-truth. (n.d.). In *Oxford Dictionaries Online*. Retrieved from https://en.oxforddictionaries.com/definition/post-truth

Public Health Watch. (2014, August 10). How a computer algorithm predicted West Africa's Ebola outbreak before it was announced. [web log comment]. Retrieved from https://publichealthwatch.wordpress.com/2014/08/10/how-a-computer-algorithm-predicted-west-africas-ebola-outbreak-before-it-was-announced/

Putnam, R.D. (2000). *Bowling alone: The collapse and revival of American community.* New York: Simon & Schuster.

Quach, K. (2016, September 29). Microsoft chatbots: Sweet Xiaolce vs foul-mouthed Tay. *The Register.* Retrieved from https://www.theregister.co.uk/2016/09/29/microsofts_chatbots_show_cultural_differences_between_the_east_and_west/

Quinn, M.J. (2014). *Ethics for the information age* (6th ed.). Boston: Pearson

Radikal. (2015, January 18). MEB veri tabanından öğrencilerin bilgileri çalınmış! *Radikal.* Retrieved from http://www.radikal.com.tr/turkiye/meb-veri-tabanindan-ogrencilerin-bilgileri-calinmis-1274727/

Rainie, L., & Anderson, J. (2017, February 8). *Code-dependent: Pros and cons of the algorithm age.* Retrieved from http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/

Rathi, A. (2018, September 17). Dealing with noisy data in data science. [web log comment]. Retrieved from https://medium.com/analytics-vidhya/dealing-with-noisy-data-in-data-science-e177a4e32621

Reiman, J. (1976). Privacy, intimacy and personhood. *Philosophy and Public Affairs*, 6(1), 26-41.

Ricterich, A. (2018). *The big data agenda: Data ethics and critical data studies.* London: University of Westminster Press. DOI: https://doi.org/10.16997/book14. License: CC-BY-NC-ND 4.0

Rosenblum, P. (2015, March 24). Bankrupt RadioShack's attempts to sell customer data meets resistance. *Forbes.* Retrieved from https://www.forbes.com/sites/paularosenblum/2015/03/24/bankrupt-radioshacks-attempts-to-sell-customer-data-meets-resistance/#79aaaa4674dd

Seaver, N. (2014). Knowing algorithms. Paper presented at Media in Transition 8, Cambridge, MA. Retrieved from http://nickseaver.net/papers/seaverMiT8.pdf

Schlanger, Z. (2014, August 11). An algorithm spotted the Ebola outbreak nine days before WHO announced it. *Newsweek.* Retrieved from https://www.newsweek.com/algorithm-spotted-ebola-outbreak-9-days-who-announced-it-263875

Schudson, M. (2015). *The rise of the right to know.* Cambridge, MA: Belknap Publishing.

Shoemaker, P. J., & Vos, T. P. (2009). *Gatekeeping Theory.* New York, NY: Routledge.

SIIA. (2017). *SIIA Issue Brief: Principles for Ethical Data Use.* Retrieved from http://www.siia.net/Portals/0/pdf/Policy/Principles%20for%20Ethical%20Data%20Use%20SIIA%20Issue%20Brief.pdf?ver=2017-09-15-130746-523

Simon, J. (2013). *Distributed epistemic responsibility in a hyperconnected era.* Retrieved from http://ec.europa.eu/%20digital-agenda/sites/digital-agenda/files/Contribution_%20Judith_Simon.pdf

Skeggs, B. (2017, September). *You are being tracked, evaluated and sold: An analysis of digital inequalities* [PowerPoint Slides]. Retrieved from: http://www.lse.ac.uk/Events/2017/09/20170926t1830vSZT/you-are-being-tracked

Slavin, K. (2011). *How algorithms shape our world* [Video file]. Retrieved from https://www.ted.com/talks/kevin_slavin_how_algorithms_shape_our_world

Sorkin, A. R., & Peters, J. W. (2006, October 9). Google to acquire YouTube for $1.65 billion. *The New York Times*. Retrieved from https://www.nytimes.com/2006/10/09/business/09cnd-deal.html

Spinello, R.A. (2011). Privacy and social networking theory. *International Review of Information Ethics, 16*(12), 41-46.

Spring, T. (2011, September 21). *How Google, Facebook and Amazon run the Internet.* Retrieved April 25, 2018, from TechAdvisor https://www.techadvisor.co.uk/feature/internet/how-google-facebook-and-amazon-run-the-internet-3304956/

Stalder, F. & Mayer, C. (2009). The second index: Search engines, personalization and surveillance. In K. Becker & F. Stalder (Ed.), *Deep search: The politics of search beyond Google* (pp. 98-115). New Jersey: Transaction Publishers.

Stodden, V. (2014). Enabling reproducibility in big data research: Balancing confidentiality and scientific transparency. In J. Lane, V. Stodden, S. Bender & H. Nissenbaum (Ed.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 112-132). New York: Cambridge University Press.

Striphas, T. (2009). *The late age of print: Everyday book culture from consumerism to control.* New York: Columbia University Press.

Striphas, T. (2010, June 14). *How to have culture in an algorithmic age*. Retrieved April 25, 2018, from The Late Age of Print https://www.thelateageofprint.org/2010/06/14/how-to-have-culture-in-an-algorithmic-age/

Striphas, T. (2015). Algorithmic Culture. *European Journal of Cultural Studies,* 18(4-5): 395-412. DOI: 10.1177/1367549415577392.

Suchman, L. (2018, June 10). Corporate accountability. [web log comment]. Retrieved from https://robotfutures.wordpress.com/2018/06/10/corporate-accountability/

Sunstein, C.R. (2001). *Rebuplic.com.* (With a new afterword by the author edition). Princeton: Princeton University Press.

Sunstein, C.R. (2007). *Republic.com 2.0.* (First edit ed.). Princeton: Princeton University Press.

Sweeney, L. (2013, April 2). Discrimination in online ad delivery. *Acmqueue, 11*(3). Retrieved from https://queue.acm.org/detail.cfm?id=2460278

Taddeo, M., & Floridi, L. (2016). The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics*, 22(16), 1575-1603. DOI: 10.1007/s11948-015-9734-1.

Tait, R. (2016, April 4). Personal details of 50 million Turkish citizens leaked online, hackers claim. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha/

Taylor, L., Floridi, L., & van der Sloot, B. (2017). Introduction: A new perspective on privacy. In L. Taylor, L. Floridi & B. van der Sloot (Ed.), *Group privacy: New challenges of data technologies* (pp. 1-12). Dordrecht: Springer.

The Guardian. (2016, March 26). Microsoft 'deeply sorry' for racist and sexist tweets by AI chatbot. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/mar/26/microsoft-deeply-sorry-for-offensive-tweets-by-ai-chatbot

The Guardian. (2018a, March 20). *What is Cambridge Analytica scandal?* [Video file]. Retrieved from https://www.youtube.com/watch?v=Q91nvbJSmS4&feature=youtu.be

The Guardian. (2018b, March 17). *Cambridge Analytica whistleblower: We spent $1m harvesting millions of Facebook profiles*. [Video file]. Retrieved from https://www.youtube.com/watch?v=FXdYSQ6nu-M&feature=youtu.be

Tonkens, R. (2012). Out of character: On the creation of virtuous machines. *Ethics and Information Technology*. *14*(2), 137-149. DOI: 10.1007/s10676-012-9290-1

Tornes, A. (2018, February 1). *Introducing the premium full-archive search endpoint*. Retrieved from https://blog.twitter.com/developer/en_us/topics/tools/2018/access-the-full-history-of-tweets.html

TrustArc. (n.d.). *What is online behavioral advertising*. Retrieved April 29, 2018, from Trust Arc https://www.trustarc.com/consumer-privacy/about-oba/#&panel1-1

Tüfekçi, Z. (2014, December 18). The year we get creeped out by algorithms. *Niemanlab*. Retrieved from http://www.niemanlab.org/2014/12/the-year-we-get-creeped-out-by-algorithms/

Tüfekçi, Z., York, J. C., Wagner, B., & Kaltheuner, F. (2015). *The ethics of algorithms: From radical content to self-driving cars*. Final draft background paper. Retrieved 15 December, 2019, from Center for Internet and Human Rights https://cihr.eu/wp-content/uploads/2015/07/Ethics_of_Algorithms_Final_Paper.pdf

Turilli, M. & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, *11*(2), 105-112.

Turkey Blocks. (2016a, October 8). *Dropbox, Google Drive and Microsoft OneDrive cloud services blocked in Turkey following leaks.* Retrieved from https://turkeyblocks.org/2016/10/08/google-drive-dropbox-blocked-in-turkey/

Turkey Blocks. (2016b, October 27). *Net internet shutdown in Turkey's Southeast: 8% of country now offline amidst Diyarbakir unrest.* Retrieved from https://turkeyblocks.org/2016/10/27/new-internet-shutdown-turkey-southeast-offline-diyarbakir-unrest/

Turkey Blocks. (2016c, December 23). *Social media shutdowns in Turkey after ISIS releases soldier video*. Retrieved from https://turkeyblocks.org/2016/12/23/social-media-shutdowns-turkey-isis-releases-soldier-video/

Turow, J. (2006). *Niche envy: Marketing discrimination in the digital age.* Cambridge: MIT Press.

Turow, J. (2012). *The daily you: How the new advertising industry is defining your identity and your worth.* New Haven, CT: Yale University Press.

Tutt, A. (2016). An FDA for algorithms. *69 Admin. L. rev. 83 (2017).* http://dx.doi.org/10.2139/ssrn.2747994

Twitter Developer Page. (n.d.). *Introducing Twitter premium APIs.* Retrieved from https://developer.twitter.com/en/premium-apis.html

Uricchio, W. (2011). The algorithmic turn: Photosynth, augmented reality and the changing implications of the image. *Visual Studies*, *26*(1), 25-35.

Uzun, R. (2011). *İletişim etiği sorunlar ve sorumluluklar*. Ankara: Dipnot.

Ünlü, N. (2016). HIV gerçeğinde kişisel sağlık verileri. H. Oğan (Haz.). *Kişisel Sağlık Verileri Ulusal Kongresi* (s. 141-146). İstanbul: Türk Tabipleri Birliği Yayınları.

Van Dijk, J. (2006). *The network society* (2nd ed.). London: Sage.

Van Otterlo, M. (2013). A machine learning view on profiling. In M. Hildebrandt & K. de Vries (Ed.), *Privacy, due process and the computational turn: The philosophy of law meet philosophy of technology* (pp. 41-64). Abingdon: Routledge.

van Strien. W. (2008). Opvangen zwakheden maakt beeldtechnieken waardevoller (interview met G.J.C. Lokhorst). Ethiek, Onderzoek en Bestuur, pp. 20-25. March 2008.

Verbeek, P.P. (2008). Morality in design: Design ethics and the morality of technological artifacts. In P. E. Vermaas, P. Kroes, A. Light & S. A. Moore (Eds.), *Philosophy and Design* (pp. 91-103). Dordrecht: Springer.

Vincent, J. (2016, March 24). Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day. *The Verge.* Retrieved from https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

Wagner, B. (2016). Algorithmic regulation and the global default: Shifting norms in Internet technology. *Etikk I Praksis – Nordic Journal of Applied Ethics, 10*(1), 5-13. https://doi.org/10.5324/eip.v10i1.1961

Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In M. Hildebrandt (Ed.). *Being profiling. Cogitas ergo sum.* Amsterdam: Amsterdam University Press, forthcoming 2019). Retrieved from https://www.privacylab.at/wp-content/uploads/2018/07/Ben_Wagner_Ethics-as-an-Escape-from-Regulation_2018_BW9.pdf

Wallach, W., & Allen, C. (2009). *Moral machines: Teaching robots right from wrong.* Oxford: Oxford University Press.

Web Archive. (n.d.). *Facts about Google and competition.* Retrieved April 10, 2018, from web.archive.org https://web.archive.org/web/20111104131332/https://www.google.com/competition/howgooglesearchworks.html

Weber, H. (2011, December 1). *Can only startups innovate? A brief history of acquisitions.* Retrieved April 27, 2018, from The Next Web: https://thenextweb.com/entrepreneur/2011/11/30/can-only-startups-innovate-a-brief-history-of-acquisitions/

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., … Schwartz, O. (2018). *AI Now Report 2018.* Retrieved from https://ainowinstitute.org/AI_Now_2018_Report.pdf

Wohn, D. Y., & Sarkar, C. (2014). The uncanny valley effect in behavioral targeting and information processing of peripheral cues. In *iConference 2014 Proceedings* (pp. 577-582). DOI: 10.9776/14075

Wu, L.L., Joung, Y.J., Lee, J. (2013). Recommendation systems and consumer satisfaction online: Moderating effects of consumer product awareness. In *2013 46th Hawaii International Conference on Systems Sciences* (pp. 2753-2762). IEEE. DOI: 10.1109/HICSS.2013.461

Yodania Group. (2016, November 23). *Google Page Rank algorithm is still alive.* Retrieved 29 April, 2018 from Yodania Group https://www.yadonia.com/blog/google-still-uses-its-page-rank-internally

Young, J. R. (2018, July 24). Why one professor says we are 'automating inequality'. *EdSurge.* Retrieved from https://www.edsurge.com/news/2018-07-24-why-one-professor-says-we-are-automating-inequality

Zarsky, T. (2013). Transparent predictions. *University of Illinois Law Review, 2013*(4), 1503-1570.

Zarsky, T. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology & Human Values, 41*(1), 118-132. DOI: 10.1177/0162243915605575

Ziewitz, M. (2016). Governing algorithms: Myth, mess, and methods. *Science, Technology, & Human Values, 41*(1), 3-16. DOI: 10.1177/0162243915608948

Zook, M., Barocas, S., boyd, d., Crawford, K., Keller., Gangadharan, S. P., … Pasquale, F. (2017). Ten simple rules for responsible big data research. *PLoS Computational Biology, 13*(3), 1-10.

Zuiderveen Borgesius, F. (2015). Informed consent: We can do better to defend privacy. *IEEE, 13*(2), p. 103-107.

Zwitter, A. (2014). Big data ethics. *Big Data & Society, 1*(2), 1-6. https://doi.org/10.1177/2053951714559253

APPENDIX 1: ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER'S THESIS ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
COMMUNICATION SCIENCES DEPARTMENT

Date: 27/02/2019

Thesis Title: Algorithmic Culture and Data Ethics

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 27/02/2019 for the total of 186 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 6%.

Filtering options applied:
1. ☐ Approval and Decleration sections excluded
2. ☒ Bibliography/Works Cited excluded
3. ☒ Quotes excluded
4. ☐ Quotes included
5. ☒ Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Date and Signature

27.02.2019

Name Surname:	Derya Güçdemir
Student No:	N14228526
Department:	Communication Sciences
Program:	Cultural Studies and Media

ADVISOR APPROVAL

APPROVED.

(Title, Name Surname, Signature)

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM BİLİMLERİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 27/02/2019

Tez Başlığı: Algoritmik Kültür ve Veri Etiği

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 186 sayfalık kısmına ilişkin, 27/02/2019 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %6'tir.

Uygulanan filtrelemeler:

1- ☐ Kabul/Onay ve Bildirim sayfaları hariç
2- ☒ Kaynakça hariç
3- ☒ Alıntılar hariç
4- ☐ Alıntılar dâhil
5- ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

27.02.2019

D. Güçdemir

Adı Soyadı:	Derya Güçdemir	
Öğrenci No:	N14228526	
Anabilim Dalı:	İletişim Bilimleri	
Programı:	Kültürel Çalışmalar ve Medya	

DANIŞMAN ONAYI

UYGUNDUR.

Prof. Dr. [illegible]

(Unvan, Ad Soyad, İmza)

APPENDIX 2: ETHICS COMMISSION WAIVER FORM FOR THESIS

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
ETHICS COMMISSION FORM FOR THESIS

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
COMMUNICATION SCIENCES DEPARTMENT

Date: 27/02/2019

Thesis Title: Algorithmic Culture and Data Ethics

My thesis work related to the title above:

1. Does not perform experimentation on animals or people.
2. Does not necessitate the use of biological material (blood, urine, biological fluids and samples, etc.).
3. Does not involve any interference of the body's integrity.
4. Is not based on observational and descriptive research (survey, interview, measures/scales, data scanning, system-model development).

I declare, I have carefully read Hacettepe University's Ethics Regulations and the Commission's Guidelines, and in order to proceed with my thesis according to these regulations I do not have to get permission from the Ethics Board/Commission for anything; in any infringement of the regulations I accept all legal responsibility and I declare that all the information I have provided is true.

I respectfully submit this for approval.

Date and Signature

27.02.2019

Name Surname:	Derya Güçdemir
Student No:	N14228526
Department:	Communication Sciences
Program:	Cultural Studies and Media
Status:	☒ MA ☐ Ph.D. ☐ Combined MA/ Ph.D.

ADVISER COMMENTS AND APPROVAL

(Title, Name Surname, Signature)

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ETİK KOMİSYON MUAFİYETİ FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM BİLİMLERİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 27/02/2019

Tez Başlığı: Algoritmik Kültür ve Veri Etiği

Yukarıda başlığı gösterilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır,
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne müdahale içermemektedir.
4. Gözlemsel ve betimsel araştırma (anket, mülakat, ölçek/skala çalışmaları, dosya taramaları, veri kaynakları taraması, sistem-model geliştirme çalışmaları) niteliğinde değildir.

Hacettepe Üniversitesi Etik Kurullar ve Komisyonlarının Yönergelerini inceledim ve bunlara göre tez çalışmamın yürütülebilmesi için herhangi bir Etik Kurul/Komisyon'dan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

27.02.2019

Adı Soyadı:	Derya Güçdemir
Öğrenci No:	N14228526
Anabilim Dalı:	İletişim Bilimleri
Programı:	Kültürel Çalışmalar ve Medya
Statüsü:	☒ Yüksek Lisans ☐ Doktora ☐ Bütünleşik Doktora

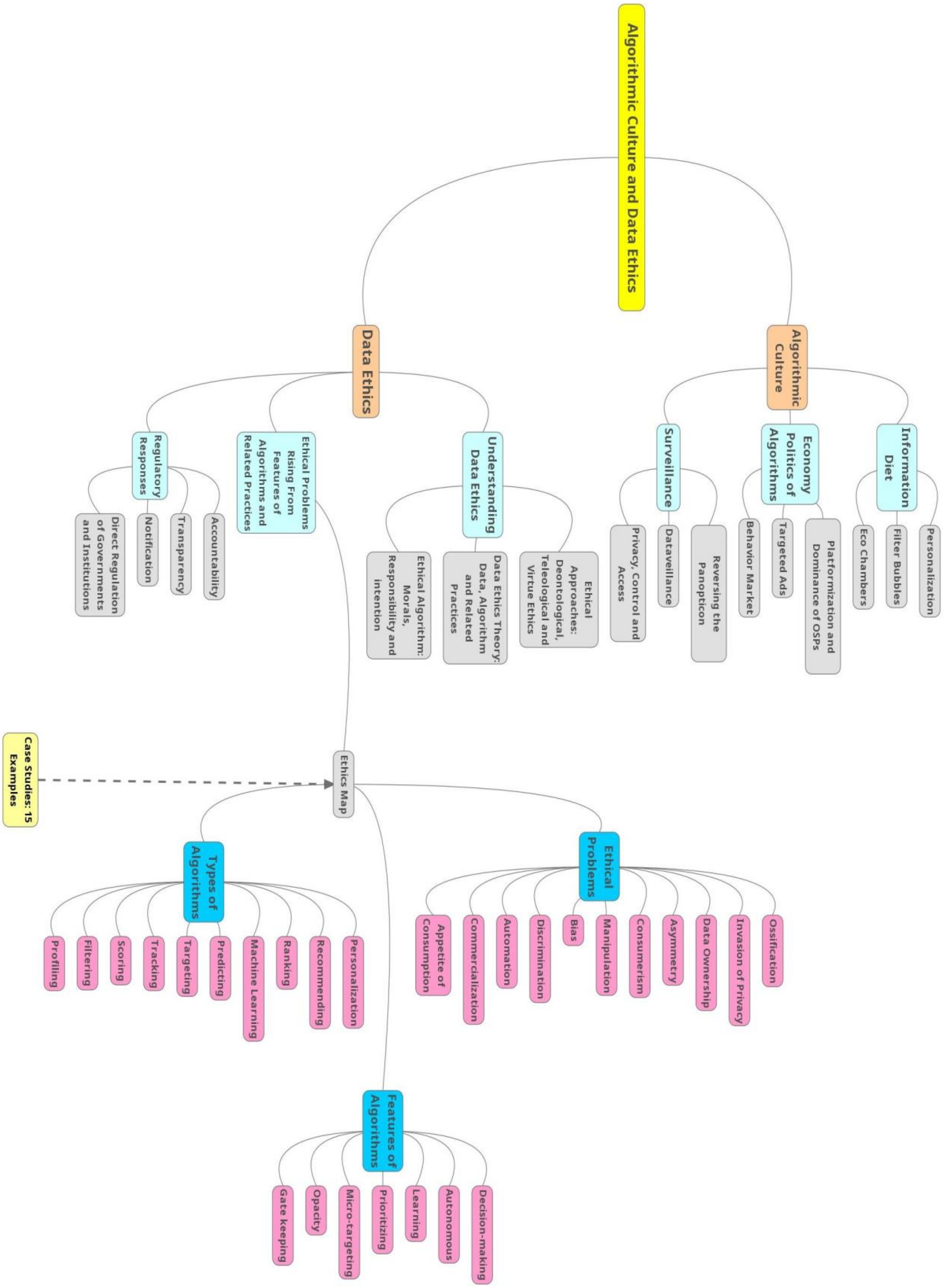
DANIŞMAN GÖRÜŞÜ VE ONAYI

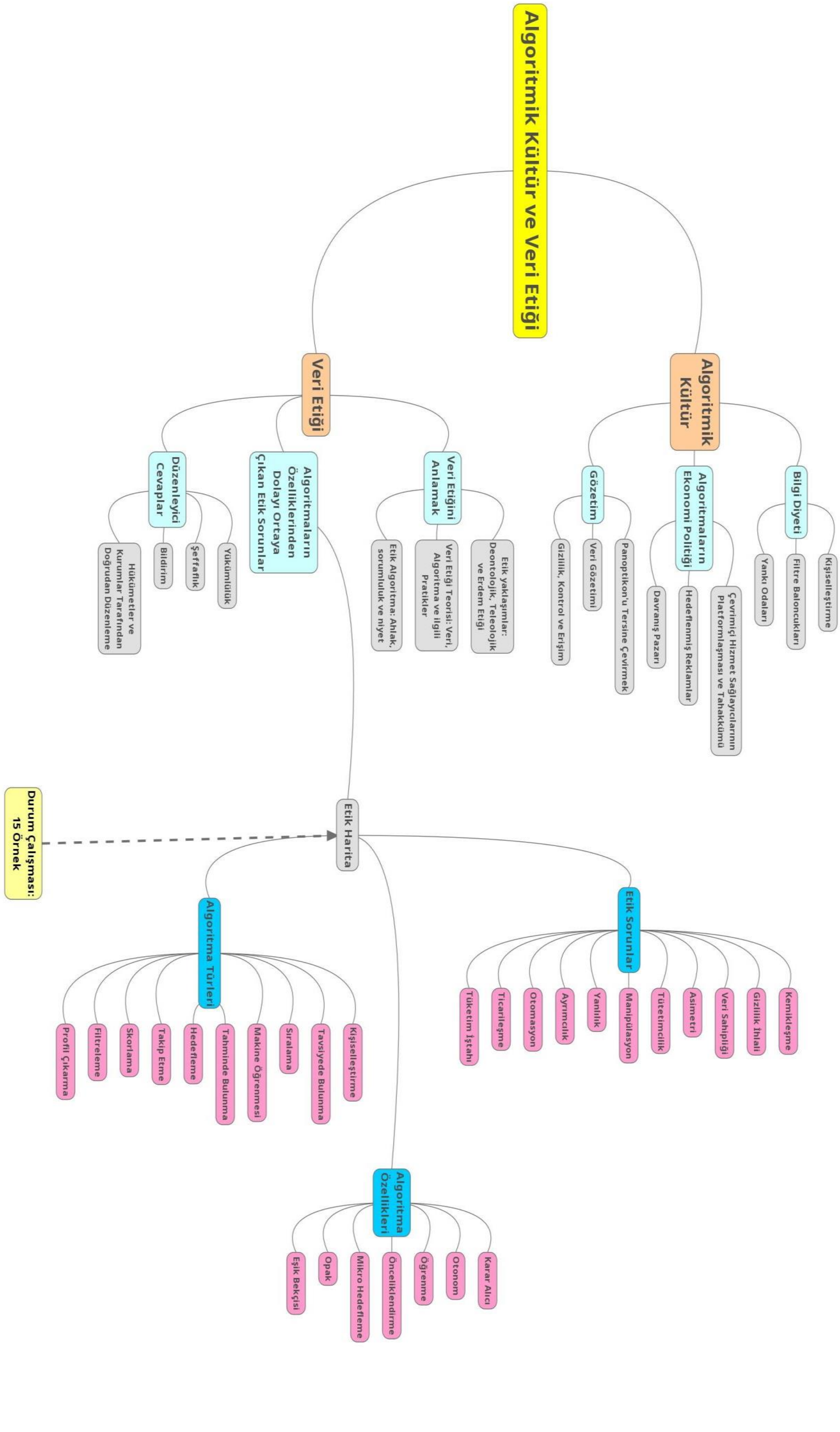
Doç. Dr. [illegible]

(Unvan, Ad Soyad, İmza)

Detaylı Bilgi: http://www.sosyalbilimler.hacettepe.edu.tr
Telefon: 0-312-2976860 **Faks:** 0-3122992147 **E-posta:** sosyalbilimler@hacettepe.edu.tr

APPENDIX 3: MIND MAP OF THE THESIS





Algoritmik Kültür ve Veri Etiği
Algoritmik Kültür
Bilgi Diyeti
Kişiselleştirme
Filtre Baloncukları
Yankı Odaları
Algoritmaların Ekonomi Politiği
Çevrimiçi Hizmet Sağlayıcılarının Platformlaşması ve Tahakkümü
Hedeflenmiş Reklamlar
Davranış Pazarı
Gözetim
Panoptikon'u Tersine Çevirmek
Veri Gözetimi
Gizlilik, Kontrol ve Erişim
Veri Etiği
Veri Etiğini Anlamak
Etik yaklaşımlar: Deontolojik, Teleolojik ve Erdem Etiği
Veri Etiği Teorisi: Veri, Algoritma ve ilgili Pratikler
Etik Algoritma: Ahlak, sorumluluk ve niyet
Algoritmaların Özelliklerinden Dolayı Ortaya Çıkan Etik Sorunlar
Düzenleyici Cevaplar
Yükümlülük
Şeffaflık
Bildirim
Hükümetler ve Kurumlar Tarafından Doğrudan Düzenleme
Etik Harita
Durum Çalışması: 15 Örnek
Etik Sorunlar
Kemikleşme
Gizlilik İhlali
Veri Sahipliği
Asimetri
Tüketimcilik
Manipülasyon
Yanlılık
Ayrımcılık
Otomasyon
Ticarileşme
Tüketim İştahı
Algoritma Türleri
Kişiselleştirme
Tavsiyede Bulunma
Sıralama
Makine Öğrenmesi
Tahminde Bulunma
Hedefleme
Takip Etme
Skorlama
Filtreleme
Profil Çıkarma
Algoritma Özellikleri
Karar Alıcı
Otonom
Öğrenme
Önceliklendirme
Mikro Hedefleme
Opak
Eşik Bekçisi