CHAPTER I

INTRODUCTION

1.1 Background

During ancient times, forms of communication have always been straightforward and unsophisticated, the medium of communication has always been so crude. The use of raw manpower has always been the norm through thousands of generations with messages being delivered through rocks and letters, carried with the use of animals or very crude modes of delivery like pigeons, dogs, horses, mules, and so forth. But in the 21st century, there has been exponential growth in the speed of how we communicate through the use of what we call the internet. The arrival of the internet has made an extreme remodel of how communications work throughout the world, especially through the effect of globalization, allowing for the cooperation of brilliant minds from across countries and continents, wherein it accelerates the growth of technology as an inflection point in the progress of humanity.

What seemed to be a never ending wait which takes days to deliver a single letter to the designated person that we wish to talk with, now becomes as easy as pressing “enter” using our fingers and the message that we want to send will be relayed in matter of seconds. These days, things such as video streaming, live streaming, and especially social media, has seeped in the bones of almost everyone, especially during Covid-19 that happened back in 2019 where everything was on

lockdown, making the virtual world of internet and social media like Google, YouTube, Instagram, Twitter, Facebook, TikTok, and so forth, feels like the only thing existing, effectively restructuring the world in a sudden to create an "Alice through the looking glass" effect. According to datareportal, an analysis from Kepios shows that 59 percent of the total global population are currently using social media, which equates to a whopping 4.70 billion social media users throughout the globe, in which over 17 famous social media has each a very bare minimum of 300 million daily active user. Social media has undergone through massive growth of user which has an average of more than 7 new users every single second spent.[1]

In Indonesia itself, the recorded active user for social media is 191.4 million in 2022 which equates to 68.9 percent of the total 100% population in Indonesia which is 277.7 million[2], where in 2021 and 2022 there has been a sharp increase of an extra 21 million citizens who are found to have used social media which in percentage equates to 12.6 percent, wherein the citizens making use of social media will spend most of their time in Tiktok, Instagram, YouTube, Facebook and WhatsApp.

But what seemed to be a positive, earth-shattering revolution to the world, has become a double-edged sword where we can feel our rights to privacy dwindling and faltering with every single second. Everyone these days could suddenly make a video of you out of nowhere and starts posting your face in the

[1]Datareportal, "Global Social Media Statistics", https://datareportal.com/social-media-users#:~:text=Analysis%20from%20Kepios%20shows%20that,of%20the%20total%20global%20population, accessed on October 16 2022
[2] Ibid.,

internet and social media, or worse, the platforms of social media that you use, that you put in your personal data, where your use it daily and it has your algorithm in whatever single thing you do, could actually violate your rights to privacy and the misuse of data, by selling your data without your consent to certain companies in order to promote their businesses through advertisement, or worse, for political purposes, whereas political campaigns are increasingly shifting their campaigning efforts of the traditional media to online platform services using the advertising tools to promote themselves more, using the advertising tools that are being offered by the tech giants such as Google, Facebook, TikTok, Twitter, YouTube, Pinterest, and so forth.

One of the reasons for the sales and purchase of this private information and data is to enable an advertising technique called microtargeting. This technique is used as a marketing strategy wherein consumer data and demographics to create a concerted and targeted effort in advertising products that is tailored to the interest[3], past purchases and viewing history of each individual consumer, thus maximizing the effect of ads through the study of the user's pattern of behavior. which of course a lot of times can violate the Privacy Rights for those individuals who don't even know that their rights to privacy has been violated.[4]

The first step to do this is usually to recognize the actions made by the people who have already use the product or service of the company, which in this

[3]Linda Tucci, "Microtargeting",https://www.techtarget.com/searchcio/definition/microtargeting, accessed on January 17 2023
[4] MNI targeted Media, "What is Micro-Targeting & How Does it Affect Advertising", https://www.mni.com/blog/advertmarket/what-is-micro-targeting-how-does-it-affect-advertising/, accessed on January 16 2023

case are the registered users on their platforms. Next, they gather data about those users, such as their sex, age, gender, education, contact information including address, phone number, and emails, and hobbies such as travel enthusiasts, pet owners, movie geeks, and so forth. Identifying these types of special characteristics will then create a perfect segmentation for a more massive audience, and create what the companies called big data. Microtargeting gives marketers big data, which then can be used to create a detailed audience profile for the advertisers. Giant companies such as Facebook sells their users data to advertisers in the form of demographics, interests, and likes. The objective of Microtargeting is to use the consumers data along with the predictive analytics to make a more profitable marketing campaign that is personalized for each users or consumer.[5]

Unfortunately, with the amount of data being taken by the companies for the use targeted ads, can also constitute to data misuse. An example, in 2019 Twitter admitted that they accidentally gave access to their advertisers about their user's personal data. The bug accidentally allowed Twitter's Tailored Audience Advertisers to have access to Twitter's users email addresses and also phone numbers. This led to the advertisers being able to give and offer the customers targeted ads without any permission outside the scope of Twitter, since the advertisers already got the user's data beforehand and could cross-reference to their own database.[6]

---

[5]Aashish Pahwa, "What is Microtargeting", https://www.feedough.com/what-is-microtargeting/, accessed on January 17 2023

[6] HNK Solicitors, "What Constitutes Misuse of Data", https://hnksolicitors.com/news/what-constitutes-misuse-of-data/#:~:text=To%20clarify%2C%20data%20misuse%20is,data%20processing%20of%20the%20company, accessed on January 17 2023.

Another example to this is Meta, where they have been fined 390 (three hundred and ninety) million euros for breaking EUdata rules regarding Article 6(1) of GDPR, trying to "bypass" the requirement for consent and processing data[7]. The problem with Meta was, according to Irish Data Protection Commission or also known as DPC, claimed that the way how Meta asked permission for their user's data for the use of ads on Facebook and also on Instagram was unlawful. The regulators stated that Facebook and Instagram cannot "force consent" their users to have to accept how their data will be used or leave the platform if they do not consent to it. The way Facebook does it is that instead of giving an option yes or no for personalized ads to their users, they just move the consent clause to the terms and conditions, and if the users do not agree, they cannot proceed to use their platform.[8]

Not only that, but Microtargeting are also usually used by politicians to target citizens in order to influence them to vote for that particular politicians[9]. Despite the debates amongst publicist, the dangers to the rights to privacy of individuals are clear based on the actions taken especially by politicians. These rights are especially challenged by the practice of online political micro-targeting, a measure commonly utilized by politicians to increase the efficacy of their online

[7] noyb,"Personalized Ads on Facebook, Instagram, and Whatsapp declared illegal",https://noyb.eu/en/noyb-win-personalized-ads-facebook-instagram-and-whatsapp-declared-illegal, accessed on January 18 2023
[8] BBC News, "Meta fined €390m over use of data for targeted ads",https://www.bbc.com/news/technology-64153383, accessed on January 17 2023.
[9] UvA, "Is political microtargeting a threat to democracy?",https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-maatschappij-en-gedragswetenschappen/news/2020/07/microtargeting.html?cb, accessed on January 18 2023

campaigns by ensuring that the targeted individuals are those especially susceptible to the campaign. Online micro-targeting in general consists of three steps:

1. The collection of personal data of the citizens;
2. from those data, identifying the groups of people who may be susceptible to the message that the politicians intend to push; and
3. after identifying the individuals, the politicians formulate tailored messages that would be more persuasive and appealing to the targeted populace.

This is done to persuade, inform, mobilize, dissuade, confuse, or demobilize voters. All forms of information can be used to identify susceptible voters and tailor the messages accordingly, including the citizens personality traits, their location, the issues they care about, the shopping behavior, and so forth, that can inform the politicians with the respective tendencies of the citizens.[10]

The Right to Privacy itself is regulated and contained in Universal Declaration of Human Rights, with most of its provisions being recognized as customary international law[11], and in the International Convention[12], with the Universal Declaration of Human Rights in Article 12 and International Conventions in ICCPR Article 17 which states that "No one shall arbitrarily interfere with his privacy, family, home or correspondence, or attack his honor and reputation.

[10] Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review, 14*(1), 82–96.
[11] European Parliament, "Universal Declaration of Human Rights and its Relevance for the European Union",
https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2018)628295, accessed on January 19 2023
[12]SFLC.IN, "Right to Privacy under UDHR and ICCPR", https://privacy.sflc.in/universal/, accessed in January 19 2023

Everyone has the right to legal protection against such interference or attacks." This right guarantees that everyone has the right to, in essence, "hide" or close parts of his life from the public eye as one of the most fundamental Human Rights.

The scope of the right to privacy under the ICCPR and the Declaration of Human Rights relates to the private life, family, home or correspondence of the individual. Being concluded in the year of 1966, the scope of the ICCPR's protection to the rights to privacy was not broad nor extensive enough to address threats to individual privacy from digital and data collection technologies, seeing as they have not yet existed at the time. The definition elaborated in the 1966 document is, therefore, considered too narrow in facing the challenges of today in regards of communications through the internet and data collection technology to be a complete regulatory provision to ensure the protection of the rights to privacy of a 21st Century individual.[13]

The right to privacy is essentially a right to obscure, hide or make disappears some parts of one's life from the public view. A person's right to privacy is seen as a fundamental human right in the wider context of international human rights law. Privacy itself can be said as an essential human right and an essential human need, thus the need for everyone to have the knowledge and information to understand that certain elements of their lives can be obscured or kept secret.

In the digital age where we are at a constant reliance to digital communications, it is questionable on whether we do have the right to conceal

[13] Kristian P. Humble, *International Law, Surveillance and the Protection of Privacy*, The International Journal of Human Rights, Vol. 25 Issue 1, 2021, United Kingdom, https://gala.gre.ac.uk/id/eprint/29182/7/29182%20HUMBLE_Human_Rights_International_Law_and_the_Right_to_Privacy_%28AAM%29_2020.pdf, accessed on October 16 2022.

ourselves, or are we part of a process that has given up the idea of privacy. The terms "privacy" can be defined in the context of personal autonomy or having innate control over personal, or intimate information or having control over personal data available to the public about oneself.[14]

At its core, privacy is about protecting oneself from the outside world. Daniel Solove, a Professor of Law from the George Washington University Law School, has put privacy into six distinct concepts:[15]

1. The right to be left alone.
2. Access is limited to an individual, which is the ability to protect yourself from unwanted access by other people.
3. Secrecy, being able to hide or conceal certain things from others.
4. Having control over one's personal information
5. Personhood, the protection of one's identity, individuality, and dignity and;
6. Intimacy, having control over or being able to limit access to one's intimate relationships or other personal aspects of life.

Solove himself put forward that by definition:

> "The value of privacy must be determined based on its importance to society, not in terms of individual rights. In addition, privacy does not have the same universal value in all contexts. The value of privacy in any given context depends on the activities of social interest it facilitates."[16]

[14] T. Gerety, R*edefining Privacy*, Harvard Civil Rights-Civil Liberties Law Review Vo. 12 Issue 2, 1977, p. 236, https://harvardcrcl.org/archive/, accessed onl October 16 2022.
[15] Daniel J. Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2009), p. 12-13
[16] *Ibid.*, p. 39

Here, Solove theorizes that privacy is something that needs to change as time goes by and perhaps also the view that what privacy means to each person varies, therefore we should not only consider the wider world's interpretation of it. This should be the basis of how the international world should see privacy. P.B Newell of the University of Warwick reiterated that privacy can be seen as "a number of different protective rights, from control over personal information, freedom from surveillance, protection from invasion of one's home, personal autonomy and control over one's body."[17]

More recently, the pre-eminent cyber law publicist Michael Schmitt has published in the Talinn Manual 2.0 that the right to privacy is highly essential in ensuring the enjoyment of human rights in the cyber context.[18] Although the extent of the protection to the right to privacy is generally known in other fields of privacy, the extent of the protection in the cyber context is still up for discussion and debate.[19] Thus, it is not surprising that experts in the field are especially torn by the implications to the right to privacy by the use of machine inspection by algorithmic analysis, a method widely used in the collection of consumer data by corporations and governments.[20]

[17] P.B. Newell, *Perspectives on Privacy*, Journal of Environmental Psychology 15 (2), 1995, p. 88-105, https://psycnet.apa.org/record/1996-14133-001, accessed on October 16 2022
[18] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), Rule 35, p. 6.
[19]G20 Leaders' Communiqué, *Antalya Summit, 15–16 November 2015; Council of Europe, Parliamentary Assembly, Resolution 2045, paras. 4, 10 (21 April 2015)*; ASEAN Human Rights Declaration, Art. 21; The Right to Privacy in the Digital Age, GA Res. 69/166, pmbl., UN Doc. A/RES/69/166 (10 February 2016).
[20] Michael N. Schmitt, *loc.cit.*, p. 8.

With the increasing amounts of collection of personal data, be it through social media, purchase of consumer goods, or as simply as viewing an article on the web, and its increasingly misuse by politicians, corporations, and criminals to the detriment of the populace, new regulations are required to prevent breaches of the rights to privacy of individuals. To combat these potentially invasive actions, some countries and international organizations have taken bold steps in attempting to regulate the processing of personal data with the ultimate goal of protecting the rights to privacy of its individuals. Amongst these nations with advanced regulations into the matter include the EU, which grants the right to protection of personal data as a separate right in addition to the right to privacy under the Charter of the Fundamental Rights of the EU (2000).

Personal Data Protection regulation first began in 1995 with the adoption of the influential Data Protection Directive. This Directive was replaced by the groundbreaking GDPR, adopted in 2016 and applied since 2018. The GDPR seeks to ensure that the personal data of EU citizens are used in a fair and transparent manner. This is done by imposing obligations upon organizations that use personal data (data controllers) and grants rights to the people whose personal data are collected and used (data subjects), wherein compliance with the GDPR is overseen by the independent Data Protection Authorities (DPA).

The GDPR is one of the most extensive regulations pertaining to protection of personal data. It applies to the processing of personal data, whose definition includes but is not limited to tracking cookies, IP Addresses, other online

identifiers, beyond the mere tangible identifiers that a person may have.[21] Aside from that, the GDPR offers wide ranging protections to personal data, even extending the protections to data controllers established outside the EU if and when they process personal data used to offer goods and services, or if they seek to track behavior of persons, within the EU.[22]

This extensive protection is encompassed under the principle of Fair Information, which have been widely adopted by states to include 120 countries in the world. This principle can be summarized to require that

1. Personal data be used lawfully, fairly, and transparently;
2. Personal data may only be collected for purposes specified in advance of collection;
3. Controllers may not collect or use data more than necessary to achieve its purpose;
4. Controllers must ensure that the data used are accurate to the persons;
5. Personal data cannot be retained for periods going beyond what is necessary for the purpose;
6. The integrity and confidentiality of the data must be ensured;
7. The controllers are responsible with compliance and any breaches of the regulations.[23]

[21] Art. 4(1), Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, (27 April 2016) (in effect as of 25 May 2018) (hereinafter as the GDPR).
[22] Art. 3, GDPR.
[23] Art. 5, GDPR.

Broadly speaking, these protections granted to the EU citizens since 2018 are highly advanced even when compared to the very recently adopted Private Data Protection Laws of Indonesia. In Indonesia, the recently ratified Law on Private Data Protection has defined Private Data to be any forms of data regarding a person which is identifiable, or identifiable when combined with other information directly or indirectly through electronic or non-electronic means.

Information here is defined broadly to mean any statement, description, thoughts, signs that contain meaning and value, messages that contain data, facts or any explanation which can be seen, heard, or read that is packaged in various forms in accordance with the development of information and communications technology be it through electronic or non-electronic means.

This law stipulates 2 (two) types of Private Data, which is private data that is general in nature, and data that is specific to each individual. General Private Data includes information such as the full name, gender, citizenship, religion, and other private information that may identify an individual. On the other hand, Private data that is specific in nature includes healthcare information, biometric data, genetic data, sexual orientation, political views, criminal record, child and family records, private finances, as well as other data specified in the Law.

This law provides protections to individuals in terms of their private data by allowing individuals to seek access regarding the identity, legal interest, purpose and usage of their private data as well as holding those that collect these data accountable. Aside from that, individuals are now able to retract their consent to

data collection, or even request the halting of any forms or processes that seek to collect and use their private information.

Aside from these *post facto* protections to data collection, the newly ratified law also requires that Agreements to collect and divulge private information contain explicit clauses that uses simple and clear language in order for it to be easily understood and distinguished from any other forms of agreements and obligations.

Here, the role of data protection laws or the law of personal data protection is needed to formulate certain legal obligations for data managers regarding storage in such a way that an individual's personal data cannot be accessed arbitrarily. This is especially important when individuals are constantly faced with advertising, be it through social media, or a simple internet search engine that displays advertisement.

Due to the increased effectiveness of targeted advertisement that utilizes private information, and the subsequent interests of corporations to use them for their own benefit, to the detriment of the consumers, it is especially important to have a robust system of laws to ensure the rights to privacy of individuals. In this vain, the writer seeks to explore the extent of data protection in Indonesia, noting the development of the laws and regulations in Indonesia, and compare them with the laws and regulations that exist in the EU, noting that they are regularly held to be the gold-standard in terms of protecting the rights to privacy of their citizens, and human rights in general.

1.2 Formulation of Issues

Based on the explanation above the Writer is interested to discuss the question:

1. How does the prevailing laws in Indonesia regulate about microtargeting?
2. How does the EU protect its users data and privacy rights in social media regarding to microtargeting in comparison with the Indonesian law?

1.3 Research Purposes

1. To know about the prevailing laws in Indonesia that regulates about Microtargeting
2. To know about the differences for social media users protection rights in Microtargeting in comparison with Indonesia and the EU.

1.4 Research Benefits

1.4.1 Theoretical Benefits

Writer wishes that through this research the theoretical benefits will grant more clarity to the reader's about the importance of Privacy Rights regarding to Microtargeting Ads, so that the reader can be more aware and be more mindful about the rights that they have, especially on national jurisdiction so that the people that live in Indonesia can have extensive and broad knowledge about the rules and regulations that have been legalized by the Indonesian government.

1.4.2 Practical Benefits

The writer expects that through the thesis that has been done and the extensive amount of research that has been made in this thesis can help the practitioners in the field understand better regarding the implementation of the law regarding to Privacy of Rights and Data Protection. And most of all to help the writer understand better, as well as to prepare for the potential practices regarding the discussion that has been discussed in the thesis.

1.5 Framework of Writing

The thesis that is being written by the Writer is arranged into five main chapters that shall make the people who read have better knowledge of the thesis.

CHAPTER I: INTRODUCTION

This chapter will discuss the introduction of the chapter that is segmented in five different parts, which are background, formulation of issues, research purposes, and research benefits.

CHAPTER II: LITERATURE REVIEW

The content of chapter II, the Writer will segment the discussion into four sub-chapters. The first sub chapter shall delve into the rights to privacy in the scope of International Laws and practices. Second chapter will elaborate into the rights to privacy in the scope of the prevailing laws, regulations and policies in Indonesia. The second to final chapter shall discuss further about the protection of data laws

and about regulations as well of the EU, namely the GDPR. The final sub chapter will delve into the data protection laws and regulations in Indonesia.

CHAPTER III: RESEARCH METHODS

In Chapter III there will be an explanation about the research type, the data analysis technique that is going to be used, and other things that the Writer will use in accordance to the issue being raised in the thesis.

CHAPTER IV: DISCUSSION AND ANALYSIS

This chapter will include discussion and analysis of the literature explained in chapter two against the current case which is the act of microtargeting on social media in the perspective of rights to privacy. The discussion will encompass rights to privacy both in the eyes of international law and the national law of Indonesia to see what they entail and how they apply to the usage of microtargeting on social media in Indonesia.

In Chapter IV, the discussion are going to be further segmented into two sub chapters, aiming to give clarity two formulation of issues raised in this thesis. The first sub chapter will elaborate further on the analysis of whether the act of doing Microtargeting actually breach any laws, regulations and policies in Indonesia with regards to the use of personal data in Microtargeting on social media with respect to the explanations provided in the literature review. The second sub chapter aims

to answer the second formulation of issue, which will analyze the data protection laws of the EU, the GDPR, and comparing it to the laws and regulations on data protection in Indonesia.

CHAPTER V: CONCLUSION

The discussion of conclusions as will give the answer to the analysis provided in chapter IV raised in this thesis. Furthermore, the Writer will also include recommendations to the concerning matter as well as potential of regulation that can be officialized and be carried through in the time ahead to help masses understand better about new policy in accordance to data protection and rights to privacy in the use of Microtargeting on social media.