# Does Human Need Privacy? : Analysis of Human Privacy in the Age of Technology

Dhita Medhavi and Ahmad Hilda Fauzi
Major of Communications, Faculty of Marketing Communications
The London School of Public Relations, Jakarta, Indonesia

**Abstract:- Freedom has been a vital aspect in humanity discourse which based on John Locke understanding of natural rights, which consist of Life, Liberty, and Property aspect (Locke, 1999). However, the advancing of technology has a significant implication towards human natural rights. For instance, it's relate to human privacy and intimacy in technological era. Through digitalization process, individual freedom had been injured massively and unconsciously (Garfinkel, 2000). Where the aspect of human privacy seemed to be disarmed without resistance. In this case, the author focused on his understanding of privacy to self-possession, integrity, and autonomy (Garfinkel, 2000). This research supported by the unauthorized used of 87 million Facebook users (Medcom.id, May 7, 2018) by Cambridge Analytica in March 2018. Indonesia as the third ranked country with the most Facebook users (Hootsuite, 2017) also feel threatened with privacy of their 1.096 million inhabitants. This research will focus on how importance the privacy status of individuals in digital era and what's social media implications on human freedom.**

***Keywords:-*** *Privacy, liberty, social media.*

## I. INTRODUCTION

Technology has provided many facilities and benefits for humanity. Efficiency, speed, and ease of information flow are one of the impacts generated from information technology. However, technology similar as a double-edged sword, can not only be used to slash enemies, but also has the ability to injure the owner. In this case, what the writer wants to emphasize is the issue of privacy that unwittingly the development of technology has limited human personal space to himself and even his fellow relations (Garfinkel, 2000). Today, information is something very valuable, where the emergence of IT technology has enabled individual personal data to be tracked, identified, and accessed freely. The development of this technology is very unsettling because it has the potential to break through the protected communication boundaries in the principles of privacy right in Indonesia.

Indonesia as a democratic country that prioritizes freedom of opinion, is important to maintain privacy in communication among the people. Especially in the digital era, concerns about monitoring of community members from irresponsible parties can lead to constructive ideas in democratic life that cannot be voiced (Carolan, 2008). This is intended to avoid any control over the privacy status carried out by the authorities, in order to limit and repress individual movement space.

When referring to the current practices of the Indonesian government, there is still no follow-up regarding the issue of violations of privacy and Personal Data Protection (PDP) against cases in the technological era where everything has been digitized. The Information and Electronic Transaction Law (UU ITE) contained in the Ministerial Regulation is still considered insufficient to prosecute cases of privacy violations and personal identity tracking on the internet and social media (Carolan, 2008).

In this case, Indonesia does not yet have standard rules with a broad scope regarding the protection of personal data in electronic systems and transactions. So far, the rules on the issue of new personal data protection are listed in the Regulation of the Minister of Communication and Information No. 20/2016. However, it is considered not strong enough to provide protection to the community, because its legal status is not stronger than the Law. Therefore, the Personal Data Protection Act (PDP Act) continues to be encouraged so that it can be immediately ratified but there are articles in the Act that can be used temporarily (Kominfo, 2018).

Without clear laws, the public cannot claim privacy that has become public consumption through digital media, which should be a basic human right (Petkovic&Jonker, 2006). Humans as units in the digital world may need to stop and think for a moment about how many people can control their personal information and where their privacy limits are. Is privacy still needed when someone in this era of digital technology? Therefore, there needs to be carefulness in understanding the private aspects of ourselves and the activities we do.

## II. WHAT IS PRIVACY?

Privacy, a term that refers to the confidentiality of information whether individual or communal. Indeed, understanding what privacy is not simple, there are many points of view and definitions of what privacy is. The understanding of privacy for sociologists is certainly different from the understanding of economists, as well as if privacy is seen from the point of view of government policy, where privacy is no longer a privilege known only to individuals.

Basically, we can say that privacy is an autonomous right of an individual, where the control of information about him is fully controlled (Diffie, Landau, 1998). This of course must be understood precisely and carefully, in order to prevent the act of privacy disarming by parties who want to use personal information as a political or business instrument. However, privacy must be interpreted as an individual's fundamental values and rights that are bound to autonomy, personal value, and independence (Waldo, Lin, & Millet, 2007). Therefore, it is necessary to recognize more about what privacy is from the point of view of scientific studies, so that it can provide a broader understanding of privacy discourse.

There are several points of view that must be understood in discussing what privacy is. As in economic studies, privacy is valued as a form of commodity or information that can be used for the benefit of market efficiency (Waldo, Lin, & Millet, 2007). Then, in the political approach, privacy is a term that is interpreted as a form of confidential information that is free from government intervention or other parties without consent (Waldo, Lin, & Millet, 2007). In contrast to the political and economic approaches, in the realm of sociology, studies on privacy focus more on mechanisms for collecting and using personal information that can reflect and strengthen power and influence relations between individuals, groups and institutions in the social (Waldo, Lin, & Millet, 2007).

There are at least 3 things that influence the shift in the meaning of privacy, namely technology, social change, and discontinuity in a country's condition (Waldo, Lin, & Millet, 2007). It is undeniable that technology is the element that has the most impact on changing the concept of privacy. Technology initiates a number of actions that are currently important and continue to be used by institutions and governments, such as the emergence of storage technology which has led to the establishment of a database of individual personal data. Speed, accuracy and efficiency are the selling points offered by this storage technology. So that the data collection process is carried out more easily.

Second, social transition, is a form of change in society with the development of technology that has changed several habituations of institutions, organizations, and social practices that are beginning to pay attention to personal data as administrative requirements. This has become an essential aspect even personal data has been converted into business sectors, such as the emergence of cyber security services. The technological movement that has infiltrated the government administration system certainly influences the bureaucratic and security system.

Third, discontinuity in a situation, this refers to the emergence of revolutionary events that can change the general perception of society about something. For example, the alleged terrorist attack caused the destruction of the WTC twin towers in America on September 11, 2011. The incident not only resulted in terror for the American people, but also brought back racial and religious issues. The whole world is beginning to be wary of every movement characterized by Arabs because of the allegation that the terrorist attacker was a member of the Al-Qaeda extremist Islamic sect. Through these events, national security is one of the priority agendas and is the vision of each country. Terrorism events also have an impact on the realm of privacy, where tapping cases against individuals begin to be done on a security basis.

Through these three things, it can be seen that our attitude in understanding the privacy problem must be based on the context that occurs. Because, it is difficult to understand privacy in just one form of perspective. Therefore, there needs to be some attitudes that can be taken when dealing with privacy issues. In this case, a policyholder must understand what needs to be formalized in the form of regulations.

Before the existence of technology, the flow of information distribution was always carried out directly without the intermediary of the device. This is done not only based on the principle of security, but also a form of intimacy on the nature of the private information discussed. However, when technology develops, individuals begin to be able to connect without needing to meet, which basically can destroy the private element in every communication that exists. This is due to the existence of a medium (third party) which is believed to be a space for individuals to share without worrying about the loss of intimate and privacy elements of a communication activity.

Nowadays it can be said that humans live in nudity, where every detail of our actions can be recorded on the basis of security. CCTV cameras in every street and building corner, track record of transactions by banking, family information, even history of cookies on websites that are used by business companies to find out our interest and activity patterns. All of these things actually lead to a process of disarmament that we unknowingly restricts individual mobility. Certainly several policies have been made in the name of personal data protection, as stated in article 28G paragraph (1) of the Constitution 1945 "The government bears great responsibility to protect the right to privacy of citizens including protecting it from all forms of threats to his personal life". The pretext is like two blades, which on the one hand can be used to maintain the integrity of privacy, and on the other hand is used to disarm privacy on a security basis.

Therefore, it is necessary to understand further how the private aspects of the individual are important and crucial in terms of their handling. This, of course, is a response to the phenomenon of digitalization which has triggered the emergence of modern privacy discourse. Nevertheless, technology is not the only trigger factor, the government with all its power also contributes to raising privacy problems. This is based on the fact that the government is a unit that has control over all data and information collected through government administration agencies.

## III. PRIVACY IN TECHNOLOGICAL AGE

The emergence of technology in human life is a symbol of ease and freedom that supports all human activities, especially in terms of communicating and obtaining information. Technological advancements that support humans to share with each other indefinitely in space and time also allow each individual to share information with the world quickly through the internet. Users of this technology can also access a variety of knowledge and services for free without the need to pay money. However, the era of technology that is progressing increasingly precisely has significant implications for basic human rights. One of them is related to the right to human privacy in the digital era (Garfinkel, 2000).

The concept of privacy is becoming increasingly important in the technological era because of the emergence of technology without being able to record and store new forms of personal information, such as fingerprints, faces and even the retina of one's eyes. Service providers like Google, for example, can find out what people are looking for and need, such as movies, music, favorite books, even where someone lives (Kemudi, n.d.).

Technology allows collected data to be tracked, identified and accessed freely so that it has the potential to violate the principles of protection of one's privacy rights (Petkovic&Jonker, 2006). A number of privacy issues also arise with the proliferation of digital technologies that unwittingly encourage people to provide personal data such as gift programs (supermarket cards, membership cards, loyalty cards) that require the collection, processing and distribution of personal data and sensitive information that should be the privacy of those who need protected.

The biggest case of privacy issues in the technology era was the leakage of personal data from 87 Facebook social media users which had been improperly shared by British political consultant Cambridge Analytica through the personality quiz application "This is Your Digital Life". The application, which was launched in 2014, is used to collect user data and map the psychological profile of people and send pro-Trump material to the downloader of the application to win Donald Trump in the 2016 presidential election (Medcom.id, May 7, 2018). Of the 87 million users, most of the misused data came from US users (81.6%) and Indonesia (1.3%).

Mark Zuckerberg at a press conference Wednesday, April 4 2018 said he accepted responsibility for the failure to protect user data and must be able to help ensure that all these elections can be held honestly and fairly, without interference or interference from certain parties who want to influence the election results through social media in the future (Jazeera, April 5, 2018). Facebook's failure to protect user data from political propaganda during the US Presidential Election is considered a threat to Indonesia. The Minister of Communication and Information (Kemkominfo), Rudiantara, warned the social media giant to safeguard users' personal data from manipulation practices and reduce the spread of false news. If not, the government claims not to hesitate to close Facebook (Artanti, April 6, 2018).

The use of the internet in the technology era allows all information to be spread in just a matter of seconds so that information theft can be wider than we ever imagined (Brey, 2006). As noted above, all types of technology have made it possible to integrate a number of sensors (cameras, microphones, biometric detectors, and all types of sensors), which are capable of capturing multiple user biometrics (face, speech, fingerprints). Consequently, people who have access can connect the biometric data with several public databases so that they can find someone's identity such as user profiles, activities, location, and behavior to the photos that can be misused (Petkovic&Jonker, 2006).

A concrete example that has occurred is the emergence of a recording from a CCTV camera that was installed at one of the ATMs owned by Bank Aceh that was uploaded to Youtube media to make a scene for cyberspace residents, especially the citizens of Banda Aceh. The video shows a pair of teenagers kissing inside one of the Bank Aceh ATMs with indecent scenes that are approximately 45 seconds from the entire duration of the video is 1 minute 57 seconds (Syah, June 26, 2015). In this case, the management of the Information Technology (IT) Bank of Aceh passed this video to the Youtube social media site on June 28, 2011 so that the public knew about it. In fact, all video recordings obtained from CCTV cameras at ATM outlets of a bank or important government agencies cannot be consumed by the public because they are confidential and privacy. The act of distributing the kiss video has violated the Information and Electronic Transaction Law (UU ITE) article 27 and article 32 (Kominfo, 2016).

Responding to the above case, indecent videos that become public consumption constitute a violation of privacy which is clearly channeled through the internet and the case is not followed up based on the privacy law in force in Indonesia. At the concept or abstract level, people understand the risks of privacy violations and the importance of privacy protection, but in practice they don't seem to care about privacy (Turow, 2014).

With internet applications that are so massive in gathering information, the key to the concept of privacy is the user's control of his personal information, respect for privacy limits and protection of that information. Unfortunately, the private sector often presents a complicated privacy policy that causes users to be reluctant to study it more deeply (Fernback&Papacharissi, 2007).

Garfinkel (2000) has also explained that "All we need to treat personal information as a property right, and then to use existing property laws to prevent unauthorized appropriation." Governments, especially Kominfo in Indonesia, need to implement and affirm privacy rights in the era digital for the community. The Institute of Electronic Frontiers Foundation in Privacy and Security on the Internet also mentions that the key to privacy is control of personal and human data that determines which information can be known to others and which are not. Even though the internet seems to facilitate digital surveillance or trace the digital footprint of each individual, it should be noted that the internet is also created with a foundation of openness and security. Practices such as tapping in the network or making the internet a closed thing are actions that injure the foundation. Maintaining the right to privacy does not only need to be based on government law, but also yourself must be more sensitive to the tools and services used when accessing the internet in this technological era (Kemudi, n.d, p. 27).

Therefore, it is necessary to understand further how the private aspects of the individual are important and crucial in terms of their handling. This is certainly a response to the phenomenon of database abuse due to digitization in modern privacy discourses. Nevertheless, technology is not the only trigger factor, the government with all its power also contributes to raising privacy problems. This is based on the fact that the government is a unit that has control over all data and information collected through government administration agencies.

## IV. PRIVACY AND THE POWER OF CONTROL

Privacy which refers to the confidentiality of information has many points of view and definitions of various studies in terms of technology, social change, and discontinuities in a state. Because privacy is not only interpreted from various angles of study, but how human efforts to fight for autonomous rights as an individual, where control of information about him is fully controlled (Diffie, Landau, 1998). The safeguarding of privacy is certainly inseparable from personal information security activities. However, what is the right way to maintain privacy, in the sense that the security of privacy can be transferred to third parties, outside of individuals who have that privacy?

As an example of a case of data leakage experienced by Facebook, we may never have thought that our interest in something could be used as valuable information. This was also done by Analytical Cambridge institutions through quiz programs that were run through the Facebook platform. Each answer from the quiz participants is used as a data source to analyze the habits and interests of Facebook users, in this case the people of the United States. Perhaps, the action was initially not too much of a problem, but after it was discovered that there was an abuse of user privacy data, the problem began to stick to the surface. The community only realized that all this time they had been directed, especially in terms of political choices that should be very confidential and private. According to the news circulating, the case was claimed to have been one of the factors of the victory of Donald Trump as the 45th president of the United States. Through the leakage of the privacy data, we could see that technology had created far more complex problems with individual privacy aspects. The existence of technology has provided a gap for parties such as website service providers, applications, software, especially the government to access and process our privacy data. This is the dilemma faced, where privacy currently seems to be monopolized on the basis of security measures. The emergence, storage and database formation technology are few of the many things that affect human privacy status, where it is done to facilitate the search and security of civil data.

Faced with database mismatches, identity theft, illegal immigration and unsolved crimes, many government policy makers put their trust in biometric identification technology (Garfinkel, 2000). This is the beginning of the emergence of data centralization of civilians. Every aspect, from birth certificate, illness history and family background, is included in a database that indirectly gives the government to monitor the private information of each individual. Private elements and security are different things that are often understood as a single meaning. This is certainly a problem when privacy issues are raised in an element of state policy. This problem refers more to the concept of privacy that until now there is still no single understanding of it. Every policy made by the state always presupposes an element of power over individuals or communals. Information becomes a commodity that can be misused at any time by irresponsible parties.

Vance Packard in one of his articles entitled "Don't tell it to the computer" criticizes how the government and agencies have invaded individual private domains through centralization and data collection (Garfinkel, 2000). He stated that:

> *"The most disquieting hazard in a central data bank would be the placing of so much power in the hands of the people in a position to push computer buttons. When the details of our lives are fed into a central computer or other vast file-keeping systems, we all fall under the control of the machine's managers to some extent (Garfinkel, 2000)"*

Moreover, currently the government has also used system biometrics to identify one's personal data. Not only physical data, but also biological data, such as fingerprints and face recognition. So that it forms an absolute identification, where the government fully has access to the data collected.

Indeed, privacy today is not about how we can hide our browsing history on the internet from our friends or family, but how the information we provide is not simply disseminated and used without consent. The privacy here is not about a thief who doesn't want to be caught by a CCTV camera, but about a couple who no longer has personal space, because they continue to feel watched. Privacy here is not about an officer with a metal detector that checks every visitor, but about someone because of his appearance as a criminal or a terrorist. Privacy is a form of self-ownership and an integral part that cannot just be harmed.

## V. IMAGINING LIFE WITHOUT PRIVACY

Privacy is a concept that is difficult to define because it deals with something subjective. Basically everyone has the desire to save some parts of life, thoughts, emotions, and personal activities are only for known to himself or his family members and closest friends. In general, what is meant by a person's domain of privacy has a different perception from person to person, from group to group, from community to community, and different according to different ages, traditions and cultures. But even though the privacy area can vary, the desire to protect privacy is universal.

The right to privacy, although not absolute rights, remains a fundamental right in the realm of human rights. What is meant by not absolute rights is when a person in a certain situation is obliged to provide very private information, but it is done to find out the problems they have experienced, such as in medical matters, and other actions that require private information. However, privacy is one of the concepts of human rights that is very difficult to define. The ease and development of technology now opens wide opportunities for the public and also the government to access and disclose information and data obtained through digital devices and internet networks. With the progress, capacity, and speed of information technology that exists at this time has high potential to violate the privacy rights of the public. This threat is mainly due to the development of information technology that is global and no longer recognizes the jurisdictions of a country.

Information disclosure and privacy protection basically have the same goal, namely to encourage the existence of accountability from the government towards the people. Therefore it is important to formulate and harmonize legislation both in terms of information disclosure legislation and for the protection of personal data, especially to have a good definition of personal information. This formulation of personal information is important to carefully formulate so as not to interfere with the interests of public information disclosure in the name of privacy protection.

## REFERENCES

[1]. Artanti, AnnisaAyu. (2018, April 6). Pemerintah Ancam Tutup Facebook. *Metrotvnews.com.* Retrieved from http://news.metrotvnews.com/metro/aNrD4w2k-pemerintah-ancam-tutup-facebook.

[2]. Carolan, Eoin. 2008. *The Right to Privacy: A Doctrinal and Comparative Analysis*. England: Thompson Round Hall.

[3]. Diffie, Whitfield. Landau, Susan. 1998. *Privacy on The Line*. United States: The MIT Press.

[4]. Syah, ArbiSabi. (2015, June 26). Bank Aceh: Antara Video Ciumandan Pelanggaran UU ITE. *Kompasiana.com.* Retrieved from https://www.kompasiana.com/ba/55017666a33311682c51035e/bank-aceh-antara-video-ciuman-dan-pelanggaran-uu-ite.

[5]. Garfinkel, Simons. 2000. *Database Nation: The Death of Privacy in the 21st Century.* United States: O'Reilly & Associates, Inc.

[6]. Hootsuite. (2018, January 14). A Long List of Facebook Statistics That Matter To Social Marketer. *Hootsuite.com.* Retrieved from https://blog.hootsuite.com/facebook-statistics/

[7]. Jaazera. (2018, April 5). 87 Juta Pengguna Facebook Terdampak Skandal Pelanggaran Privasi. *Beritasatu.com.* Retrieved from http://sp.beritasatu.com/home/87-juta-pengguna-facebook-terdampak-skandal-pelanggaran-privasi/123496.

[8]. Kemudi. n.d. Privasi & Kemanan di Internet. *Kemudi.xyz.* Retrieved from https://kemudi.xyz/static/web/modul/[lores]%20modul%204%20EBookModulKEMUDI.pdf

[9]. Kominfo. 2018. Undang Undang Republik Indonesia Nomor 19 Tahun 2016. *Kominfo.go.id.* Retrieved from https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf

[10]. Locke, John. 1980. *Second Treatise of Government*. USA: Hackett Publishing Company, Inc.

[11]. Medcom.id. (2018, May 7). Data Disalahgunakan Pengguna Tetap Percaya Facebook. *Medcom.id.* Retrieved from https://www.medcom.id/cards/11161-cambridge-analytica/GbmjJ13k-data-disalahgunakan-pengguna-tetap-percaya-facebook

[12]. Papacharissi, Zizi& Gibson, Paige L. 2007. *Privacy Online: Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites*. United States: Springer Publishing. Retrieved from https://pdfs.semanticscholar.org/c536/fb5c027feeddebcd97c26e4426e0f0e3637c.pdf

[13]. Petković, Milan &Jonker, Willem. 2006. *Security, Privacy, and Trust in Modern Data Management*. United States: Springer Publishing.

[14]. Turow, Joseph. 2014.*Americans and Online Privacy: The System is Broken.* United States: Penn Library. Retrieved from https://repository.upenn.edu/cgi/viewcontent.cgi?article=1549&context=asc_papers

[15]. Waldo, James. Lin, Herbet S. & Millet, Lynette I. 2007. *Engaging Privacy and Information Technology in A Digital Age*. Washington DC: The National Academies Press.