SDGs, Privacy and Gen-Z: Preliminary Studies on Technological Awareness in South Sumatera Senior High School Students

Farisha Sestri Musdalifah[1], Muhammad Yusuf Abror[2], Miftha Pratiwi[3], Muchammad Yustian Yusa[4]
{mifthapratiwi@fisip.unsri.ac.id[3]}

Universitas Sriwijaya, Indonesia[1, 2, 3, 4]

Abstract. This paper aims to explain the increasing awareness of technology security for adolescent privacy which is currently dominated by Gen Z. Technology is part of human innovation that has become a necessity for the industry as an infrastructure in facing the challenges of industry 4.0. As stated in the Sustainable Development Goals, the 17 goals agreed upon by 193 countries at the United Nations. The technology sector is included in the focus of goal number 9, which is about industry, innovation and infrastructure. The rapid use of technology in various countries has not been accompanied by awareness of privacy security. Indonesia is one of the countries that supports the implementation of SDGs in accordance with Perpres No. 59 of 2017. One of the accelerations in achieving the SDGs is the use of information and communication technology. This research was conducted on high school students in Sekayu, South Sumatra. Aims to reveal the level of awareness of adolescents about the threat of data privacy through smartphone technology. Some applications and programs downloaded on smartphone can access personal data on the cellphone. The results showed that awareness of the threat of spreading privacy through smartphones used by Gen-Z adolescents is still low.

Keywords: SDGs, Technology, Privacy, Youth

1 Introduction

Information and communication technology is the main thing for modern humans today; therefore, it is a daily necessity. This is important for the photo on the objectives of the Sustainable Development Goals (SDGs) program launched by the United Nations and 193 other countries. The SDGs themselves have been campaigned around the world since September 25, 2015 and right in 2016. It has 17 goals to make all countries connect and accelerate one of them is Indonesia. The program so that the 17 goals proclaimed by the SDGs run smoothly, the government made a legal umbrella in the form of Presidential Decree No. 59 of 2017. Awareness of technology is the 9th goal in the SDGs program, namely regarding infrastructure, industry, and innovation. Information and communication technology is included in target 9.c, which includes indicator 9.c.1* regarding the population served by mobile broadband; 9.c1. (A) regarding individual representatives controlling/owning mobile phones; 9.c.1. (B) represents individuals using the internet (Bappenas, 2017). With the targets and indicators contained in goal 9 of the SDGs and also the goals of the Indonesian

ICISPE 2020, October 09-10, Semarang, Indonesia

DOI 10.4108/eai.9-10-2020.2304815

government, increasing access to information and communication technology is accompanied by data protection for its users so that it is not misused by irresponsible parties.

This is because there are still technological devices that can be seen from people carrying out data hacking activities and technology users who use technology carelessly so that privacy data hacks occur which can be misused. However, in this study the authors focus on the awareness of the use of smartphone technology connected to the internet, especially for school teenagers.

The development of information and communication technology, which is increasingly prevalent, makes all information easily accessible via the internet. Based on the survey results from the Indonesian Internet Service Providers Association, the penetration of internet users in Indonesia is 64.8%, where internet access is carried out using smartphone devices from various brands. Today, smartphones have become a necessity for humans to be able to communicate with other humans. In our daily lives, smartphone have an effect on business, education, access to health, entertainment and socialization [1].

However, the use of information and communication technology is not necessarily accompanied by an awareness of the threats from privacy and personal data that we enter into our smartphone. Today's technology enables invasive data and privacy. These data can be collected into one big data unit, so that it can be used to read human behavior [2]. One of the Big data services is for business purposes, namely to read consumption behavior in society. Have you ever filled in personal data such as full name, telephone number, email address, or city of residence to get a discount or discount? If so, then that is one of the ways marketers gain data on their consumers.

Data invasion is also very possible through the presence of malware (malicious software), especially for smartphone users with the Android operating system, where the operating system is open source [3]. Malware itself is a program designed to disrupt systems, collect privacy-causing information, and can illegally access system resources “US-CERT Control Systems Security Center” [4]. In other words, the user's personal data can be retrieved and there is the possibility that it can be misused for certain purposes.

In addition, every cellphone user unconsciously and unconsciously shares his privacy on the internet, especially through social media. The APJII [5] survey states that the three main reasons for using the internet include communication, social media, and seeking work-related information . In social media, the movement of users must be more selective in what is carried out by the public. Utilization of social media features such as checking locations and uploading photos that have an impact that threatens internet privacy.

Awareness of the dangers of this privacy threat can vary according to age, age internet users are not aware of the practice of personal data [6]. The young age group, especially adolescents today, is a generation that grows up with technology. One of the young age groups is high school adolescents, the age range is around 14-18 years. Many teenagers are already familiar with smartphone from the elementary school level, but they do not yet realize how important it is to maintain privacy in using smartphone. Therefore, academically this research tries to fill the empty space regarding privacy awareness for smartphone users among teenagers, especially high school students in the Sekayu District, Banyuasin Regency, South Sumatra Province.

2 Literature Review

The term privacy is often equated with anonymity, even though privacy and anonymity are two different terms. Privacy is not an attempt to hide something from the outside world, nor is it an activity to close oneself off from society. Over time, in this 21st century computerization era, privacy has become one of the human rights. The human rights referred to here are the rights for a person to control what things are allowed and cannot be released into the public sphere. In the context of this research, the internet and social media are also included in the public domain.

In order for internet users to run safely, data protection from the government is needed. For example, what has been done by the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines to accommodate the protection of personal data [7] and the protection that has been carried out by countries in Europe under the auspices of the European Data Protection [8]. Thus, apart from not being active, the responsibility for data privacy lies with internet users, the government must also provide active data protection. Often personal data in Indonesia is leaked, such as through e-commerce, even from government agencies themselves.

Various websites visited by internet users will also store personal data. Usually, internet users will be asked to enable cookies and this will read basic data such as email address and name, so that search engines can see patterns from internet users and display advertisements according to user habits. Like Google, which owns Google AdWords, indirectly controls which ad networks are displayed to users [9].

A state based on law uses law as the main foothold or is called the rule of law, so it must not ignore three basic ideas of law, namely justice, benefit, and certainty [10]. Thus, government administrators should provide these three basic ideas to provide data security for internet users.

3 Methodology

The methodology in this study uses a way of dissecting it with literature studies that are used as a basis for thought and concept to be able to answer the cases that the author studied. The concept used in the research is the concept of human security which is based on the fulfillment of human rights so that they can achieve what they want and avoid threats to themselves [11]. So that the hacking of personal data is a threat that should be protected by both national and international law. This is related to human security which must be protected by the state. The humans who are threatened are humans who are not free. Free here is freedom in using the internet calmly without having to fear that your personal data is threatened from hacking and data misuse.

In addition, it also used a survey method to 40 students at SMAN 1 Sekayu, Rahmaniyah SMA, SMKN 1 Sekayu, and MAN 1 Musi Banyuasin, Sekayu City, Musi Banyuasin Regency, South Sumatra Province through purposive random sampling technique. The 4 schools represent 40 students, each consisting of 10 students. All high school students are in the Z Generation category. According to the Pew Research Center, generation Z is the generation born after 1996. The survey became the core of this research so that students could understand the level of understanding of the threat of privacy in using their smartphone technology in everyday life.

4 Results and Discussion

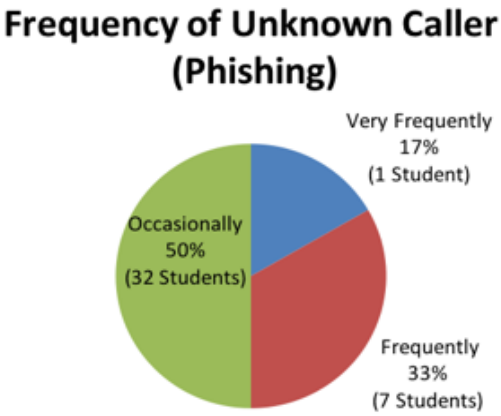
Privacy is a person's right to be alone and this right is recognized as the basis of human rights by the United Nations Declaration of Human Rights [12]. So, privacy becomes important to discuss because it is part of human rights that must always be protected. Some examples of privacy breaches include data mining, being targeted by the market, and harassment from unwanted people. For example, suddenly there are pop-up ads on smartphone or search pages which are actually quite annoying. In addition, there are short messages from unknown numbers offering various goods, services, and even online gambling. Deeper than that, there are scammers who directly call cellphone users. Of course, this is very unsettling and disturbs the privacy of technology users.

So, the urgency to immediately ratify the Personal Data Protection Bill is important. The bill that provides criminal sanctions ranging from 1 year to 5 years with fines from twenty billion to 70 billion can provide a sense of security for internet users, as well as a big warning to rogue individuals and hackers who steal personal data.

The increase in the use of short messages is increasing and is dominated by teenagers [12]. So that it makes them not separated and away from technology which includes a short message feature. If we refer to Graeff & Harmon's [6] writing which states that young internet users are more aware of data privacy, then this needs to be reviewed again. Especially young internet users in small areas or cities. Can it still be concluded that young technology users are sensitive and aware of their privacy or even ignore the safety of their personal data?

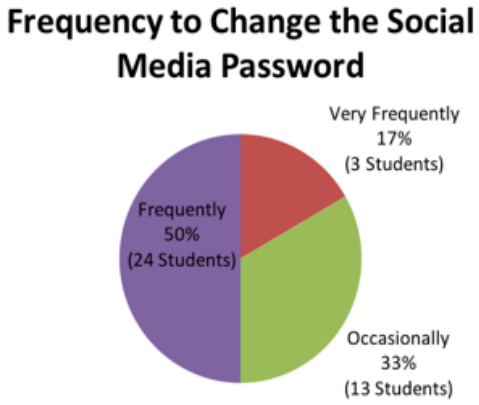
This study wants to see how the level of awareness and understanding of young internet users who come from areas or small cities of personal data. So that the authors made observations through a survey conducted in the city of Sekayu Musi Banyuasin. And distributed to 40 students from SMAN 1 Sekayu, SMA Rahmaniyah, SMKN 1 Sekayu, and MAN 1 Musi Banyuasin. In the research that has been conducted, it has found that not all students in the city of Sekayu have a level of awareness of data privacy.

One method of hacking data is phishing, where the perpetrator / foreigner calls the target by asking for various information related to privacy and data security, such as: full name, place of birth date, name of biological mother. The survey results obtained showed that 32 students did not often (occasionally) receive calls from strangers. Meanwhile, 7 students receive calls frequently and only 1 student receives calls from strangers very often.

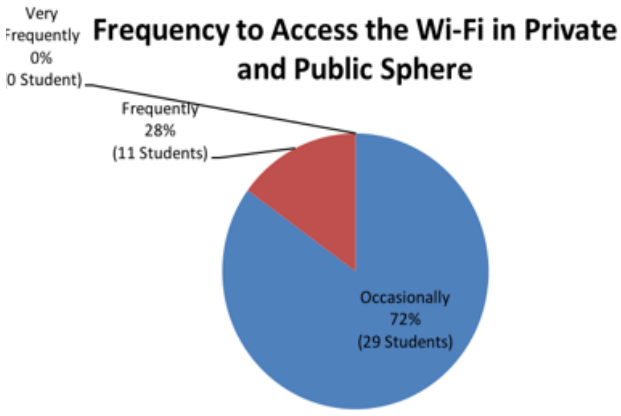


Seeing the above phenomena, recommendations for action to be taken are to raise students' awareness of the importance of personal information. This information is vulnerable to abuse by irresponsible people through phishing schemes.

The next finding was that around 24 students changed their keywords frequently while 13 students did not change keywords frequently.



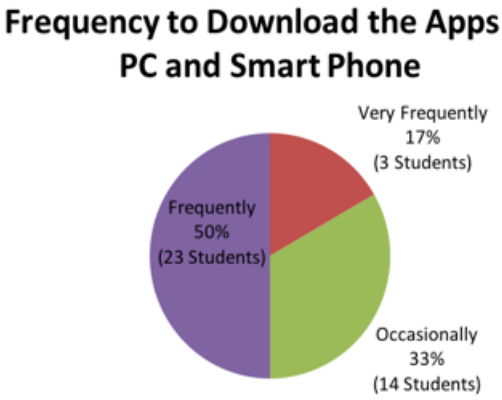
The frequency of changing the password for access to social media on a regular basis is quite important to protect the security of student data. Therefore, changing social media keywords periodically must always be done. Especially if you access / log in from public places, such as internet cafes, public Wi-Fi, which creates the potential for password breaches through keystroke logging or key logging schemes. Admins or hackers have prepared software on the PC that functions to record what is typed by the keyboard. As a result, when typing keywords, personal data is automatically stored in the key logging software and has the potential to be misused.



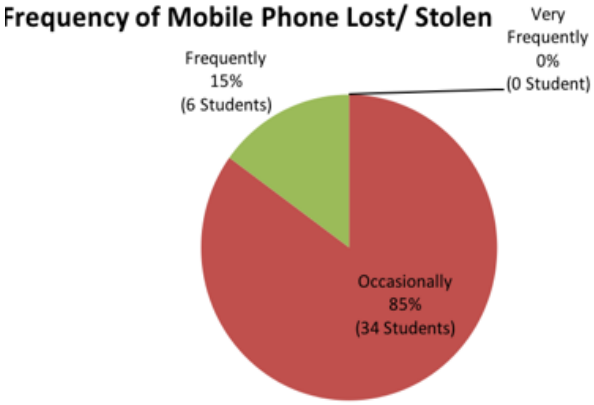
The frequency of accessing devices through private and public places indirectly creates vulnerabilities to data security. As explained above, public access has the potential to create threats from third parties (crackers) who will hack account passwords and other sensitive information. The data obtained shows that there are 11 students who frequently access Wi-Fi

from public places and 29 students who do not frequently access from public places. Anticipation that can be done in the future is when public Wi-Fi areas have started to spread to the village, then awareness to always protect data by constantly changing keywords regularly must be a priority.

Data security is also related to the frequency with which applications and software are downloaded on a smartphone or PC. When a user downloads an application, there is a kind of Terms of Condition that asks the user to "allow" the application/application developer to access personal data, such as: contacts, photos and others.



The data above shows that 23 students (50%) of SMA / MA students in Musi Banyuasin Regency often download applications, and there are even 3 students who frequently download applications up to 20 applications. On that basis, continuous socialization efforts are needed to students, so that they are aware of the potential dangers of downloading applications frequently. This is reinforced by reports and news that discuss smartphone applications that have been infiltrated by malware and spyware that can steal personal data of application users.



The frequency of losing a smartphone can also be a source of leakage of personal data. There are 6 students out of 40 students who often lose their smartphones. As is well known, in these smartphones there must be data that is quite important, such as social media accounts to

short messages. There is a protocol that must be run when you want to replace a new cellphone. Instead of selling old cellphones or transferring them to someone else, it is better if the cellphone is destroyed by burning. This is because even though user data has been deleted, the data recovery software will make the lost data come back.

Nonetheless, periodic socialization is needed about the importance of destroying old cellphones so that it will raise awareness that cellphones are consumables and cannot be renewable.

Based on this research, it can be concluded that not all internet users among adolescents at the SMA/SMK/MAN level in the city of Sekayu have an awareness of the privacy of their data contained in personal cellphones. Thus, the role of the government as a regulator is also needed to immediately enact a law on personal data protection. This is so that the security of people's personal data can be guaranteed and well protected.

References

[1] M. Sarwar and T. R. Soomro, "Impact of smartphone's on society," *Eur. J. Sci. Res.*, vol. 98, no. 2, pp. 216–226, 2013.

[2] S. Stephens-Davidowitz and A. Pabon, *Everybody lies: Big data, new data, and what the internet can tell us about who we really are*. HarperCollins New York, 2017.

[3] Z.-L. ZENG, Y.-T. NI, and B.-G. LIN, "Permissions Based Android Malware Stealing Privacy Data Detection," *DEStech Trans. Comput. Sci. Eng.*, no. iceit, 2017.

[4] U. S. C. E. R. Team, "'US-CERT Control Systems Security Center.' (T. Nash, Ed.) Retrieved 2020, from US-CERT Control Systems Security Center," 2005. .

[5] T. APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indonsia," *Jakarta Diambil dari https//apjii. or. id/content/read/104/348/BULETIN-APJII-EDISI-22---Maret-2018. Tanggal*, vol. 22, 2018.

[6] T. R. Graeff and S. Harmon, "Collecting and using personal data: consumers' awareness and concerns," *J. Consum. Mark.*, 2002.

[7] W. Raymond, "Privacy, A Very Short Introduction." Oxford University Press, 2010.

[8] A. Lukács, "To Post, or Not to Post-That Is the Question: Employee Monitoring and Employees' Right to Data Protection," *Masaryk UJL Tech.*, vol. 11, p. 185, 2017.

[9] D. Cherry, *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online*. Syngress, 2013.

[10] Badan Pembinaan Hukum Nasional, *Naskah Akademik RUU Perlindungan Data Pribadi*. 2016.

[11] L. S. M. Gunawan, M. P., *Kantor Menteri Negara Lingkungan Hidup: Proyek Agenda 21 Sektoral, United Nation Development Program (UNDP); Indonesia. 2000. Agenda Pariwisata Untuk Pengembangan Kualitas Hidup Secara Berkelanjutan. Proyek Agenda 21 Sektoral,*. Jakarta: Menteri Negara Lingkungan Hidup dengan UNDP, 2000.

[12] G. Danezis, R. Clayton, A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, "Digital Privacy: Theory, Technologies, and Practices." Auerbach Publications, Boca Raton, FL, 2008.