

Indonesia Digital Rights Situation Report 2019

The Rise of Digital Authoritarian



SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

July 2020

The Rise of Digital Authoritarian Indonesia Digital Rights Situation Report 2019

Composing Team

Person in charge : Damar Juniarto

Coordinator : Anton Muhajir

Information Acces Team : Unggul Sagena, A. Ryan Sanjaya, Abul Hasan Banimal, Aseanty Fahlevi, Supriyono

Freedom of Expression Team : Ika Ningtyas, Nenden Sekar Arum, Bimo Fundrika

Digital Security Team : Ellen Kusuma, Nike F. Andaru,

Design and Illustration : Daeng Ipul

Translators: Supriyono & Bani Nawalapatra

Southeast Asia Freedom of Expression Network (SAFEnet)

Jl Gita Sura III no 55 Peguyangan Kaja

Denpasar, Bali 80115

Phone: +628119223375

E-mail: info@safenet.or.id

Website: safenet.or.id

Table of Content

Introduction	1
About SAFEnet	3
Summary	5
Case Data	
• Right to Internet Access	9
• Right to Freedom of Expression	19
• Right to Feel Secure	27
Epilogue	45

Introduction

Indonesia's 2019 Political year has passed, but its leftovers are felt until this year. Presidential Election that supposes to be a celebration and fair contestation in democracy, has been marked with cross disputes including in the digital world. That helped color the situation of internet freedom in this country during 2019. The leftovers of the presidential election disputes are felt among others in the occurrence of the Internet blackout in 2019 and the rampant criminalization using articles in the Information and Electronic Transaction Law (UU ITE).

Disputes between the 2019 presidential elections become one of the important records of the digital rights situation in Indonesia over the past year. Nevertheless, violation of digital rights in Indonesia also happened because of other reasons, like social environment conflict, especially in the regional area. Citizens are either criminalized or their right to security are violated because of their activity on overseeing public services.

The dynamic of political situation has caused the increasing violation of digital rights in 2019 compared to previous years. Data from Indonesian National Police shows that for the past 3 years, the number of internet-related cases handled by the police keep increasing from 1.338 cases in 2017 to 2.552 in 2018, and 3.005 until October 2019.

The increasing of criminalization against citizen related to their activities on the Internet in 2019 has become one of the records that continues to repeat from year to year. It is the same in silencing of the critical voices of citizens who express and argue through the Internet, especially social media. Activists and journalists are most of the victims, besides the emergence of new victims, especially academics.

Previously, SAFEnet recorded various violation of citizen digital rights through a yearly report, a tradition that we started a year ago. However, we changed the title of the report from *Yearly Report* to *Indonesia Digital Rights Report*. This change we consider is necessary to better reflect the contents of the report itself as well as introducing the issue of digital rights.

The Southeast Asia Freedom of Expression Network (SAFEnet) has been paying attention to the issue of digital rights since 2018, five years after the network was founded and initially only advocated for freedom of expression online. In general, these digital rights include the right to access the Internet, the right to express using digital media, and the right to feel secure in digital media.

This report is an attempt to not only record the various violations of digital rights that happened during 2019, but also place them in a bigger context, as of how they impact democracy. As a new terminology, digital rights have not received serious attention, including how these rights are closely related to the more fundamental rights, human rights (HAM).

We arrange this report with 3 methods. First, collection of data from reports that come directly to us during 2019, especially for criminalization case and gender-based violence online (KBGS). Second, collection from secondary sources like the police department and courts that are open for the public, like on their website. Third, through media monitoring.

We divide the structure of the report in 3 different main areas related to digital rights, namely rights to access internet, rights for freedom of expression using digital media, and rights to security in the digital world. This deviance is not rigid as one or two cases can be correlated so that they can be placed in more than one section. This is also to show how each part of digital rights is closely related one another as a whole.

Aside of being a tool to introduce digital rights issue, we hope this digital rights situation report can be our advocacy in pushing the country to create fulfillment and protection to the digital rights. Happy reading.

Denpasar, July 2020



About SAFEnet

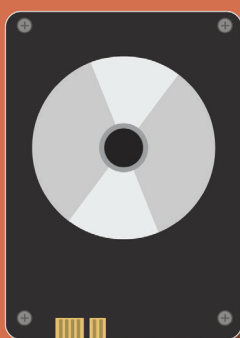
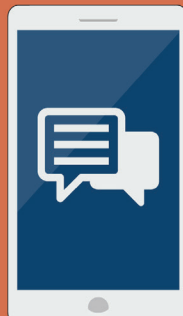
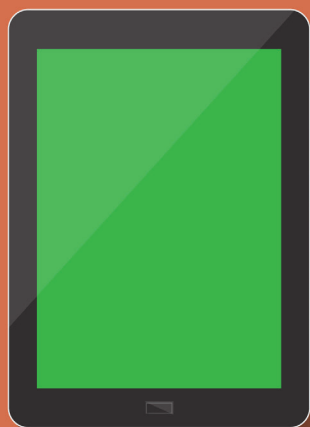
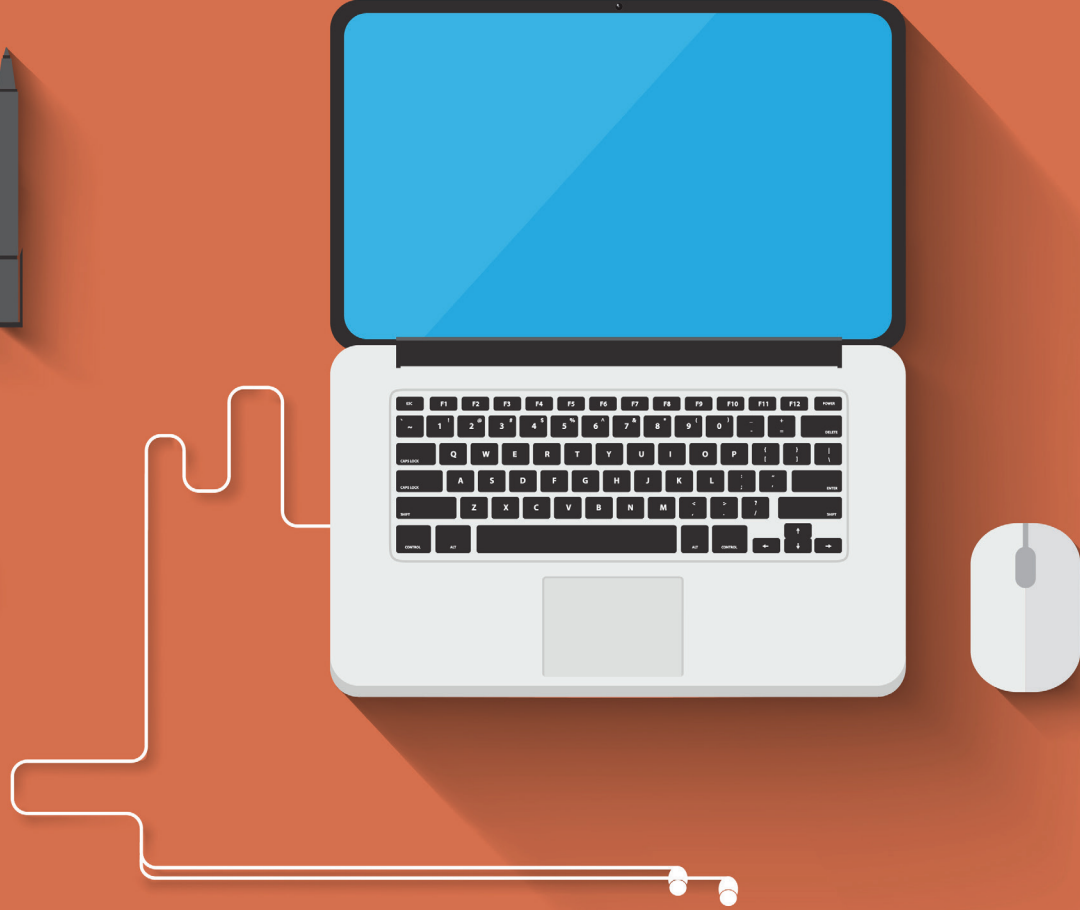
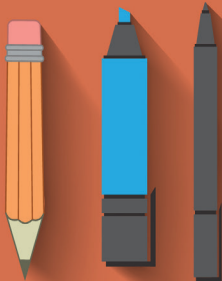
Southeast Asia Freedom of Expression Network (SAFEnet) is digital rights defender network in Southeast Asia that was found on 27 June 2013 in Bali. In January 2019, SAFEnet officially incorporated with the name of the Association of Southeast Asian Freedom of Expression having its domicile and office in Denpasar until now.

The founders of SAFEnet consisted of a blogger, journalist, internet governance expert, and activist. It was established following the rampant criminalization of netizen because of their online expression after the enactment of Law (UU) Number 11 of 2008 concerning Information and Electronic Transactions (ITE). Although this law was later revised to Act No. 19 of 2016, criminalization of citizens remains rampant.

In 2018 SAFEnet started widening the issue of advocacy to the direction of digital rights; earlier it only focused on advocacy for freedom of expression online. That is because of the increasing issues related to the Internet from the perspective of human rights (HAM). Not only the right to freedom of expression but also the right to access the Internet and the right to security.

Currently SAFEnet has around 40 volunteers spread across 23 cities, including Pekanbaru, Pontianak, to Papua. These volunteers monitor many cases related to digital rights, campaigning the importance of digital security rights, and building public capacity on fighting for digital rights.

These activities aligned with SAFEnet main programs that are (1) Monitoring violation of digital rights, (2) Giving advocacy on the policy level and helping victim for accessing justice, along with (3) Building supports, solidarity, and connection in between digital right defenders in Southeast Asia and especially Indonesia.





Summary

We ever experienced euphoria, where Internet and social media could be a room to flourish the freedom of society and encouraging the birth of civil society that was based on democracy. There was freedom, equality and citizen sovereignty. The euphoria was manifested, among others, by the mushrooming of Internet-based community movements as a balancer and supervisor of power that tends to be authoritarian.

More than one decade had passed by after the birth of many social media, like Facebook and Twitter, which also became a catalyst for community movements including in Indonesia, this euphoria fades away. The freedom in internet that we experienced, keep getting limited day by day with many kinds of justification and patterns. The equality that we once celebrated, now under dystopia. The sovereignty of digital rights that we have not yet fully achieved, is now completely taken away.

It is depressing but that is how it is.

The tendency of the past year shows that digital rights in Indonesia, which we have only been able to enjoy for the past decade, are now under the threat of authoritarian rule. The documentation of the situation of Indonesia's digital rights that we carried out over the past year supports this thesis.

Like the Internet infrastructure supporting it, digital rights are one interconnected link that start from right to access, right to freedom of expression, and right to security. First, citizens should not only be free to access the Internet, but even guaranteed its right to obtain the same access without having to insulate the location and demographics. Second, each citizen should freely express their opinion without having to fear of being threatened. Third, without being threatened, every citizen will find a safe and comfortable shared space in the digital world.

Unfortunately, the situation in the past year has been far from ideal.

Termination of Internet Access

During 2019, there were three times of Internet shutdowns in Jakarta and other parts of Indonesia (no clear data available for the regions in detail) on 22-24 May 2019, then in Papua and West Papua on 21 August 2019, and on 23- 29 September 2019 in Wamena and Jayapura.

Limiting and blocking the internet access in Jakarta and other parts of Indonesia in May 2019 are related to demonstrations in response to the results of the 2019 presidential election. During these three days, the government officially conducted an internet outage or Internet throttling to “prevent hoax” and as the “Anticipatory steps for conflict to not expand” and “maintain order and security”.

The termination of Internet access in Papua and West Papua is closely related to demonstrations against racism on Papuan students in Surabaya and Malang, East Java. The government has slowed access in several areas of West Papua Province and Papua Province, including Jayapura City, Jayapura Regency, Mimika Regency, and Jayawijaya Regency and Manokwari City and Sorong City.

Internet Shutdown become a new pattern taken by Indonesian government besides blocking more access to certain website and application. This policy is a new pattern to violate rights against internet in the name of national security as also happened in the region of Rakhine (Myanmar), Kashmir (India), and Catalan (Spain).

Internet shutdown as the new pattern for limiting access to internet complements the old challenges of affordability of internet access in Indonesia, location,

demographic, and gender gap. From local side, Internet in Indonesia at 2019 still concentrated more in Java with 55%, followed by Sumatera 21%, Papua 10%, Kalimantan 9%, meanwhile Bali and Nusa Tenggara have the smallest internet user with only 5%.

In terms of gender, internet access in Indonesia is still marked with the digital gap where 72% of adult men have cell phones, while adult women only at 64%. The cellphone users who access the Internet are 43% men and 36% women.

Criminalization against Expression

When internet access keeps getting limited through many ways, including cutting down access, and facing the old problem that still have not finished, like digital gap, at the same time, the user facing repeated threats facilitated by articles in the ITE Law. The documentation along 2019 shows that criminalization against online expression continues to occur.

From report submitted to SAFEnet, there were 24 criminal cases that related to the ITE Law. That number decreased compared to cases last year which reached 25 cases. From the background of the victims, media and journalist dominated the figure with 8 cases, consisting of 1 media and 7 journalists being the victims. Over the past 2 years, the amount of media and journalist that were convicted with the ITE Law tends to be higher than the previous years.

The second most victims were activists and residents (5 cases). This number is up 1 case compared to the previous year. The remaining victims include educators and artists with 3 cases each.

From the aspect of article, Article 27 paragraph 3 of the ITE Law (Defamation) is the most used to report the cases (10

cases). Followed by Article 28 paragraph 2 (Hatred) with 8 cases. The use of two articles at a time is also reported three times in Article 27 paragraph 1 (Pornography) along with Article 27 paragraph 3. As well, one case used Article 27 paragraph 1 with Article 28 paragraph 2.

These two facts show a connection that journalist, activist, and vocal citizen are the most criminalized with using articles that can be interpreted in many ways with the aim of silencing critical voices. The thesis then was supported by another fact that it turns out that the background of the accusers who used the articles most are public officials and politicians with 10 reports.

Another thing to watch out is the extended background category of victims of criminalization using the ITE Law. Over the past year, there has been increasing criminalization against academics whose voice are critical against national political issues or in their universities.

Even so, the data we collected is only the tip of the iceberg of the actual number of cases. In comparison, according to the Directorate of Criminal Acts at the Indonesian National Police Headquarters, the number of investigations of social media accounts has always increased every year, namely 1,338 cases in 2017, 2,552 cases in 2018, and soar to 3,005 cases until October 2019. Of all the 3,005 cases until October, the most complaints were insults to public figures, authorities and public organization with 676 cases.

From the figure, most of the investigations involved public figures, authorities and public organization. In 2017, there were 679 cases being investigated in connection with insults, increased to 1,188 in 2018, but then decreased in 2019 to 676 cases. Other upper cases are the alleged provocation and hate speech.

These 3 cases often refer to the use of articles on the ITE Law. The involvement of catchall articles on the Internet Law continued throughout the past year.

A More Gripping Threat

After restrictions on access and the threat of criminalization, Internet users in Indonesia must also face increasingly strong digital violence, especially against critical voices towards authority and women.

From July 2019, SAFenet has been working with the National Commission for Women (Komnas Perempuan) recording all the cases of cyber-violence based on gender. Throughout 2019, SAFenet receive 60 complaint cases on criminalization case and gender-based violence online (KBGS) in which 44 of them were from the National Commission on Violence Against Women reference in SAFenet. The 16 other complaints were filed in through SAFenet communication channels, including those directed by partners or other communities to make their complaints recorded at SAFenet.

From the figure, 53 victims are women and 7 others did not specify their gender. The most reported forms of KBGS are nonconsensual dissemination of intimate images (45 cases), privacy violation (Like doxing, non-sexual surveillance, tapping, access without authorization) with 7 cases, an impersonator account (2 cases), showing off their genitals in digital spaces without approval (digital exhibitionism) with 3 cases, and other form like shaming victims on public digital spaces (online shaming) or violating victim privacy outside the description above.

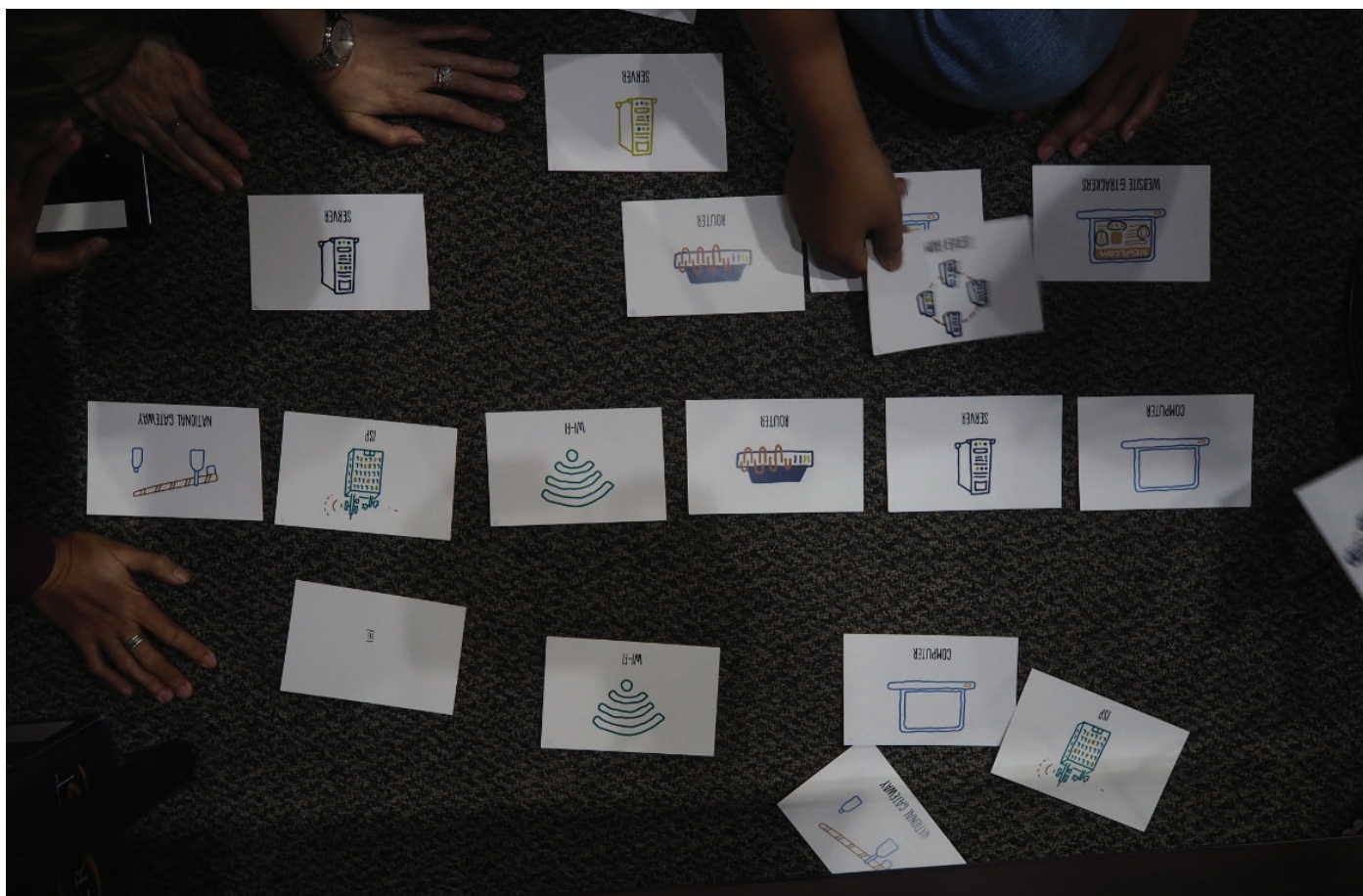
The cases of KBGS above did not always occur in one form. There are also several forms of violence that happen at once. Like spreading the victim private data without consent online. In term of the platforms used, it is not only one social

media platform, but many others at once. For instance, not only on instant messenger, but Twitter, Instagram and Facebook too.

Just as with internet access restriction and criminalization toward users, violation toward security too happened because of political motivation. At first, cases of KBGS happened more because of revenge from couple or ex-couple and inequality between men and women. However, 2019 marked the start of the KBGS with political motivation. A female activist becomes a victim through the distribution of her nude pictures from her work partner who was an activist too. The distribution of the material was an effort to delegitimize their work in rejecting the revision of the Corruption Eradication Commission (KPK) law.

The politicization of the female body as happened to activists who rejected the revision of the KPK Law is a sign of how the Internet has become a tool for power to silence the critical voices of citizens through various means. Not only restricting and even interrupting Internet access or threatens with the criminalization of their political expressions, it also perpetrates cyber-based violence for political purposes.

If all the digital rights violation in the country are left untouched, then Internet freedom that we once wish as a progress in Indonesia is only a matter of time before being buried again.



RIGHT TO INTERNET ACCESS

Internet in Indonesia

There is no precise data on the exact figure of internet users in Indonesia by 2019. But several sources suggest it is around 120 to 175.4 million. According to *Data Reportal*, until January 2020, the number of internet users in Indonesia reached 175,4 million, with an additional of 25 million or 17% compared to the previous year. Internet penetration in this country reaches around 64% of the population. The same source said, the number of social media users in Indonesia reaches 160 million until January 2020, an increase of 12 million or 8,1% between April 2019 to January 2020¹.

Other data from Association of Indonesian Internet Service (APJII) said the number of Indonesian internet users

by May 2019 is 171,1 million, increased by 10% from the previous year which was 143,26 million. The penetration reached 64,8% percent². Most of them access Internet from mobile devices, like cellular phone, tablet, and laptop. Even, the number of mobile users exceeded the number of users themselves that is 338,2 million or 124% from total population.

According Statista Dossier only 14% users subscribed to home internet (fixed internet subscription), however 97% home internet users access it from phone device too³. As for the utility, it is still dominated by the need for short messages through Internet based platforms and social media⁴.

² <https://dailysocial.id/post/pengguna-internet-indonesia-2018>

³ <https://www.statista.com/statistics/1036571/indonesia-fixed-internet-subscription-at-home/>

⁴ <https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/>

¹ <https://datareportal.com/reports/digital-2020-indonesia>

Internet Access: Geographic, Demographic, and Gender

According to the APJII survey results, until the end of 2018, internet access still focused on Java (55,7%) then Sumatera (21,6%), Sulawesi, Papua, and Maluku (10,9%), Kalimantan (6,6%), and Bali and Nusa Tenggara (5,2%). Beside demographics, there are still gaps in Internet access where only 20.3% of smallholders use the Internet in Indonesia. This compared with, for example, factory workers, 71.6% of whom use the Internet or the State Civil Apparatus which reaches 89.9%. As for the reason they do not use the Internet is because they do not know how to use it.

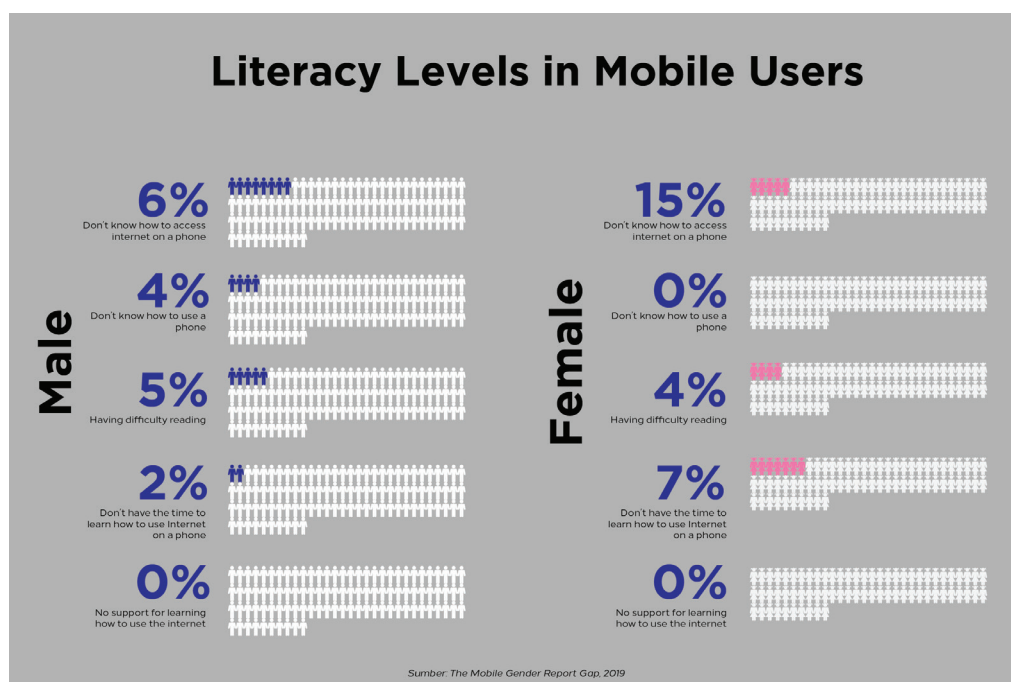
In terms of age, APJII documented that the highest penetration of Internet users came from the age 15-19 by 91%. Followed by the age group of 20-24 (88.5%) and the age of 25-29 (82,7%). The lowest penetration is the age group of 65 and above (8.5%).

From all these age groups, there are no recorded comparisons between male and female users, but according to 2019 GSMA yearly report, Indonesia still experiences digital disparities based on gender; 72% of adult male have a phone, while 64% of adult female have it. Interestingly, not every person that uses a phone has access the Internet. Mobile users who access the Internet are 43% in men and 36% in women.

The issue above is caused not only

because of the limited infrastructure provided, but also because of level of literacy. Gaps in the level of internet literacy in the gender of female and male are shown in the following table:

Table 1. Literacy Levels in Mobile Users



Unfortunately, in the midst of the widening digital divide between Java and outside Java, there has also been a violation of the right to access the Internet which is actually very limited, for example the blackout of the Internet in Papua and West Papua.

Polemic on Internet Shutdown

In the context of rights to access information, a case that becomes main attention in Indonesia is the occurrence of internet shutdown. In this case, the Indonesian government uses several terms to name the internet shutdown like Internet Throttling, “Hoax anticipation”, “Accelerating the security recovery process”, “Riot prevention” and many other phrases, which in essence are still same as the Internet shutdown which violates human rights.



Simply, the internet restriction is an intentional disruption toward internet-based communication, that cause disability on accessing internet. Termination on Internet access can be done on certain populations, locations or services with the aim of controlling the flow of information. It can occur at the national level or at certain regions and users.

During 2019, Internet shutdown happened 3 times; on 22-25 May 2019 in the form of bandwidth throttling to slow down pictures and video transmission on WhatsApp and social media platform in Jakarta and several other cities in Indonesia. Then in 19 August - 8 September 2019, a bandwidth throttling happened for 2 days and followed with an internet shutdown for almost 3 months in Papua province and West Papua. The last was on the 23 - 28 September 2019 internet shutdown in Wamena, Papua. All three incidents have the same motivation namely politics.

The blocking and slowing down internet access on May 2019 happened after the demonstrations against the announcement of the presidential election result, precisely on 22-24 May 2019. In these 3 days, the government officially did an internet shutdown by showing and introducing the term of Internet Throttling officially to the public with the purpose of "Preventing hoax" and as "Anticipatory steps for conflict so as not to expand" and "Maintain order and security".

The excuse of maintaining order and security caused many problems within the society. The internet restriction made the journalists difficult to verify their journalistic products in the field or citizens to verify the information to his relatives including those who participate in the demonstration, as well as causing the one way and monopolistic information from the government.

The second incident in August 2019 was later seen as a pattern which will be common to be taken by the government. During the period, the government shut down the internet in Papua for 338 hours after multiple demonstrations and riot happened in several cities in Papua and West Papua. Protest happened in the form of peaceful demonstration, though some (if not most) of them turn violent, in respond to racial discrimination to the Papua students in Surabaya and Malang. The slow handling of cases of racial violence by law enforcement has led to demonstrations in various regions.

Instead of thoroughly investigating racist and violent perpetrators against Papua students, including in Malang, 15 August 2019 and in Surabaya on 16 August 2019, the Ministry of Communication and Information (Kemkominfo) chose to slow down the internet on 19-21 August 2019, followed by the internet shutdown on 22 August to 8 September 2019 under the pretext of preventing the spread of false information in Papua and West Papua. Similar reasons are carried out continuously, based on the guidance that in addition to government version of information, other version of information can be labeled hoax or fake news. While actually this case was not that simple.

Details of Internet shutdown are as follows. First, the government slowed internet access in several areas of West Papua Province and Papua Province on 19 August 2019 from 13:00 WIT until 20:30 WIT. The second internet shutdown was when the government deliberately blocked data services and/or terminated every internet access in Papua Province (29 cities/districts) and West Papua Province (13 cities/districts) dated 21 August to at least 4 September 2019 at 23:00 WIT.

Table 2. Internet shutdown in Indonesia in 2019

No.	Location	Time	Perpetra- tor	Reasons and Description
1	The whole Indonesia	22 – 25 May 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ <i>Bandwidth throttling</i> restricting access on social media and apps ▪ Anticipatory steps for conflict to not expand ▪ Limiting the spread of hoax
2	Papua Province and West Papua	19 August – 8 September 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ The reason is “... speeding up the process of restoring the security situation ...” (Source: Kompas.com) ▪ Internet access blocked for 2 weeks (Sumber: CNNIndonesia.com) ▪ Internet shutdown for 338 hours. (Sumber: vice.com)
3	Wamena City and parts of Jayapura	23 – 29 September 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ It was carried out during the riots in Wamena and parts of Jayapura city ▪ Reason: Limiting the spread of hoax and preventing widespread riots

Meanwhile the third internet shutdown was extending to the blocking of data services and/or termination of internet access in 4 cities/districts in Papua province (Jayapura City, Jayapura district, Mimika district, and Jayawijaya district) and 2 cities/districts in West Papua Province (Manokwari City and Sorong City) since 4 September 2019 23.00 WIT until 9 September 2019 18.00 WIB/WIT.

Throughout 2019, Indonesia experienced internet shutdown for 416 hours. The total estimated losses incurred due to these actions were reported at 187,7 million USD, or around Rp 2,5 trillion⁵.

Internet outage was not carried out through open and participatory mechanisms. All the government's excuses are only unilaterally determined without showing the principles of accountability. This has led SAFEnet and other network organizations to protest these actions, including through online petitions and lawsuits.

⁵ <https://www.top10vpn.com/cost-of-internet-shutdowns/>

China's Domination In Indonesia Digital World

One crucial issue related to the digital rights in the last 5 years is the strengthening of China's dominance in Indonesia's digital world, from hardware, software, to digital business. In hardware, for instance, after South Korea's Samsung dominated Indonesian market for so long, now China is slowly dominating, through its made-in China products.

Based on Statcounter GlobalStats data, sales of smart phones in Indonesia during May 2019 – May 2020 dominated by Samsung, OPPO and Xiomi. All of three consistently maintain market-share above 15% for a year. As a unit, Samsung still dominated quarter of total smartphone sales in Indonesia, at 24,91% in May 2020 and 25,93% in May 2019.

Meanwhile, products from China like OPPO and Xiomi compete for the second and third ranks. In May 2020, OPPO was in second rank with market-share of 20,62%, increased from 18,6% in May 2019. OPPO experienced a significant jump on its sale in November 2019, followed by a steady increase in the following months until finally replacing Xiomi's position at second place in January 2020. Xiomi has a market share of 19,8% in May 2020, decreasing from 21,07% from May 2019, making it ranked third in May 2020.

For Chinese product with market-share category under 15%, Realme, Huawei and Lenovo have a market-share of respectively 3,72%, 1,05%, 0,83% in May 2020. From the three of them, Realme

is a product that has experienced a rapid increase in a year in which it was initially at the bottom with 0.03% in May 2019, rising significantly to 3.72% in May 2020.

In general, China dominates almost half of the smartphone market-share in Indonesia with 46,02% in May 2020. It increased by 3,3% from 42,7% in the same month of 2019. China's dominance in the smartphone market share in Indonesia is caused by the variants of products that are served to Indonesian consumers, which are many, compared to other foreign countries.

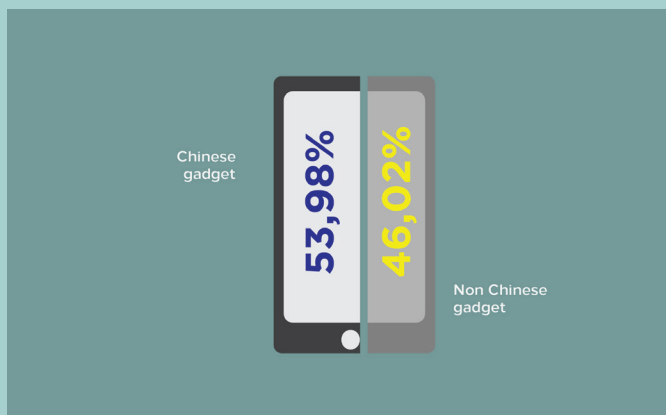
Meanwhile, other source claims that Chinese smartphone vendors controlled 75% of total smartphone shipments in Indonesia, in the third quarter-2019.¹

Smartphone Marketshare in Indonesia

Name of Product	Origin Country	May 2019	May 2020
Samsung	South Korea	25.93%	24.91%
OPPO	China	18.6%	20.62%
Xiomi	China	21.07%	19.8%
Mobicel	South Africa	7%	11.4%
Apple	United States	5.51%	7.86%
Realme	China	0.03%	3.72%
ASUS	Taiwan	4.12%	2.97%
Unknown	-	7.78%	2.88%
Huawei	China	1.13%	1.05%
Lenovo	China	1.87%	0.83%

Source: [Statcounter GlobalStats](#)

¹ News is accessed on the link <https://tekno.kompas.com/read/2019/11/18/17080077/merek-china->



The high supply of *Made in China* smartphone in Indonesia has been illustrated by the change of value of imported telecommunication equipment from China. In 2007, imported telecommunication products from China tripled from the previous years, then continued to explode until no other imports from other country can chase after them. As an illustration, it could be seen in the following graph.

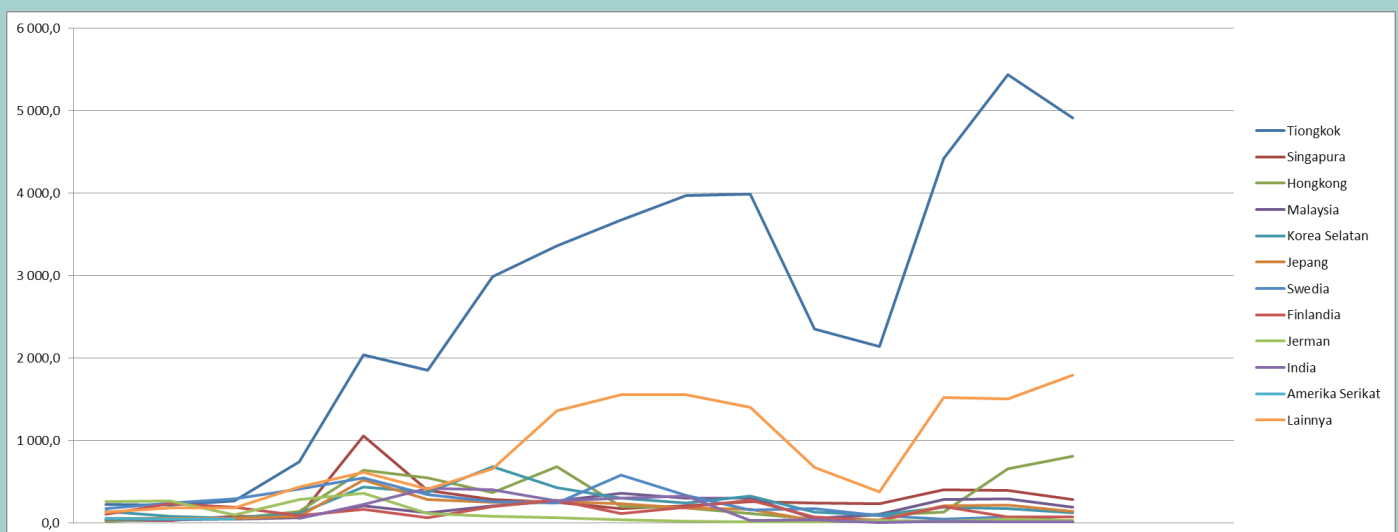
[kuasai-75-persen-pasar-smartphone-indonesia](#)

Smartphone Application

Unlike hardware, software from China still has difficulty to compete with other products from other country. This could be seen from the number of ratings and usage of smartphone applications in PlayStore in Indonesia which until June 2020, is still dominated by United States products, like WhatsApp, Instagram, Twitter, YouTube, and so on. These applications dominate not only in the number of its downloads, but also usage.

In term of number of downloads, there are only 4 Chinese applications that make into the top 20 in Indonesia, that is TikTok (Rank 3), SHAREit (Rank 5), Mobile Legend (Rank 8) and Lazada (Rank 18). Meanwhile in usage, there is only one application from China that make into the top 20, namely UC Browser in rank 17.

That being said, there is a sign that penetration of software from China slowly started to become alternative in Indonesia. In January 2020, Bank Indonesia issued a permit for WeChat Pay to operate in Indonesia. WeChat



Electric Equipment Import 2002 – 2019
Source: BPS¹

1 Data can be seen in <https://www.bps.go.id/statictable/2014/09/08/1049/nilai-impor-perengkapan-telekomunikasi-menurut-negara-asal-utama-nilai-cif-juta-us-2002-2019.html>

Pay is a payment platform, that is developed from Chinese instant messaging application WeChat. They were finally able to enter Indonesia in collaboration with the CIMB Niaga Bank network. Its rival application that also came from China, Alipay, is said to have been processing its permit to operate in Indonesia. Alipay will cooperate with Bank Central Asia network.

This is in accordance with the China rules regarding the restriction of cash carried by the tourists. Other than that, more than 90% citizens of Chinese big cities have used WeChat Pay and Alipay as their payment method.²

Data Security Issues

Globally, the use of made-in China digital applications is another big issue, especially for the United States (US) which has been in trade war with the country in the past years. This concern arises because of the potential security risks of the Chinese products for both users and a country. The Chinese technology company that is currently 'in war' with the US is Huawei.

Huawei is a company that provides the telecommunication tools and services in the world, in which its technology is developing fast. It currently prepares the 5G network technology, which is seen by the US as an entry point for Chinese intelligence to take action to spy on the US government. As a result, Huawei became one of the companies blacklisted by the US government. US President Donald Trump has reportedly limiting the supply of components to Huawei.

West countries, especially United State, accusing 5G devices developed by Huawei have a backdoor that can be used by the Chinese government to do surveillance so that they can spy the condition of

certain country. Though that accusations were strongly denied by Huawei and the Chinese government, Huawei product and services have been rejected by many countries including United State, Australia, New Zealand, England, Japan, France and German.³

In January 2019 the US Department of Justice reportedly filed criminal charges against Huawei and its finance director, Meng Wanzhou.⁴ The US demanded 23 charges against Huawei, starting from cases of theft of T-mobile technology to deceiving the US into doing business with Iran

There are speculations in the global realm that digital products from China are said to have weaknesses in terms of security based on the assumption that Chinese products are allegedly always under the shadow of the Chinese government, so that they can be used as a tool for espionage. A related issue that became the topic of discussion was the 5G device infrastructure is now developed by Huawei, as the leader and owner of the largest patent in 5G devices.⁵

Huawei in Indonesia

Huawei has started their business in Indonesia since 2000 by selling communication equipment and consultancy service. As digital infrastructure vendor, Huawei with the help of their partners now serving around 500 clients in multiple sectors, including the government, infrastructure company, and many more. Huawei hopes in the future to work closer with the health and beauty sectors to help digitize their systems.⁶

Other than that, Huawei too already pocketed several applications from

2 Information could be read in <https://katadata.co.id/berita/2020/02/12/wechat-pay-alipay-diyakini-tak-akan-rajai-pasar-dompot-digital-lokal>

3 <https://www.thejakartapost.com/news/2018/12/18/huawei-defends-global-ambitions-amid-western-security-fears.html>

4 Information could be seen in <https://www.bbc.com/indonesia/indonesia-47037816>

5 <https://www.cnbcindonesia.com/tech/20200611133719-37-164647/saat-donald-trump-tidak-berdaya-di-hadapan-huawei>

6 <https://www.thejakartapost.com/adv-longform/2019/08/27/huawei-helps-create-win-win-digital-ecosystem-in-ri.html>



oppo vivo



Indonesia that have been registered to its AppGallery, a platform that launched by Huawei as an alternative for Google Play and App Store. In January 2020, AppGallery already have 40 Indonesian digital apps in the banking sector (Permata Bank, BCA Mobile, Link Aja) and e-commerce (Blibli, Tokopedia, Bukalapak). Huawei targeted that there would be 73 digital applications from Indonesia registered in AppGallery by March 2020.⁷

Not only in the digital business, Huawei also takes part in the sector of national security. In October 2019, The Indonesian Cyber and Code Agency (BSSN) collaborated with Huawei in strengthening cyber security in Indonesia through developing the human resources of BSSN employees.⁸ However, even though Huawei is accused of having the potential to endanger security, BSSN stated that there is nothing to worry about this collaboration because it was only related to HR development. BSSN dismissed concern that this cooperation is a form of taking side on one country and ignoring another. On the contrary, it instead emphasizes that BSSN acts neutral as in 2018, the agency too worked together with a US company, Cisco.⁹

Regarding the practice of 5G network in Indonesia, Ministry of Communication and Information is currently reviewing the frequency. Government hopes Kutai Kartanegara as the country's new capital city to be the first to use it. There is no certainty when 5G will be implemented in the country, but according to the Indonesian Telecommunications Services Providers Association (ATSI) this network can be implemented starting in 2022.¹⁰

Although the 5G network has not entered Indonesia yet, in 2020 there have been four types of smartphones that support 5G technology officially circulating in Indonesia. All of them are mobile phones from China namely OPPO Find X2, OPPO Find X2 Pro, and Huawei P40 Pro.¹¹ In addition, three Indonesia's Internet network providers namely Telkomsel, XL Axiata and Smartfren have conducted a test for the 5G network.^[12]

[13]

Seeing Indonesia's enthusiasm in welcoming the 5G network, it is important to underline the issue of digital security as alleged by the United States and its allies. Although there is no explicit evidence of the allegations, at least there must be caution in implementing this 5G network in the country. The Indonesian government must ensure whether this issue is true and make preventive measures in case the US allegations of the 5G network turn true.

7 <https://www.thejakartapost.com/news/2020/02/28/huawei-aims-to-have-73-local-indonesian-apps-in-appgallery-by-march.html>

8 <https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber>

9 <https://www.cnnindonesia.com/teknologi/20191029154752-185-443825/gandeng-huawei-bssn-sebut-tak-perlu-khawatir-isu-spionase>

10 <https://katadata.co.id/berita/2020/03/09/indonesia-dianggap->

[siap-adopsi-5g-tahun-depan#:~:text=Mereka%20pun%20memperkirakan%2C%20nilai%20bisnis,1%2C83%20juta%20pada%202025.](#)

11 <https://www.suara.com/tekno/2020/05/14/155348/daftar-ponsel-5g-ini-sudah-masuk-pasar-indonesia?page=1>

12 <https://inet.detik.com/telecommunication/d-4802327/telkomsel-sukses-uji-coba-5g-di-batam>

13 <https://teknologi.bisnis.com/read/20190822/101/1139774/uji-coba-5g-smartfren-lebih-cepat-xl-axiata-lebih-menarik>



RIGHT TO FREEDOM OF EXPRESSION

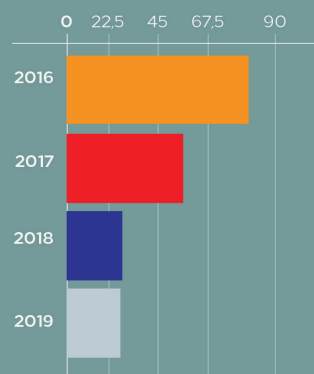
Criminalization of Journalist and Activist Remains High

Convictions toward the right to freedom of expression using the articles in the ITE law still occur throughout 2019, which coincides with the political year. From data collected by SAFEnet, there were 24 cases of criminal convictions with the ITE law, decreased from 2018 which was only 25 cases.

Based on profession of the accused, the media and journalists still stood in the first position with 8 cases, consisting of 1 media and 7 journalists being victims. In the last two years, the number of convictions against media and journalists tends to be higher than in previous years.

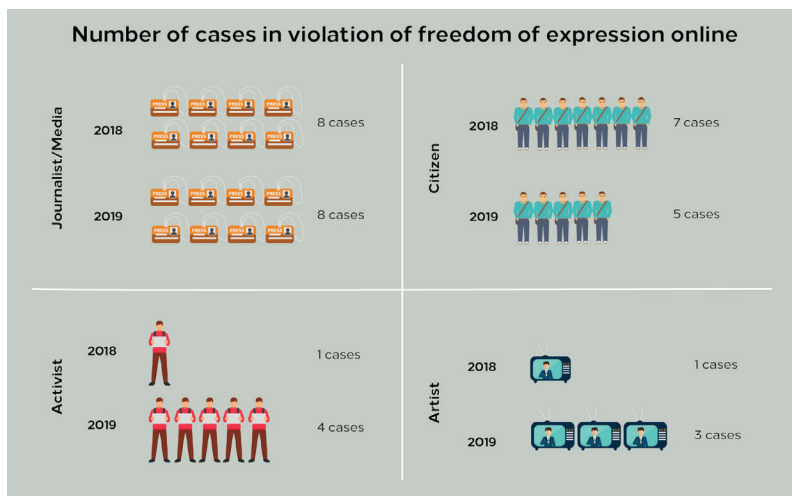
In the second position, criminalization of the right to expression also happened to activists and citizens with five cases in each category. The number of criminal acts against activists increased from previously which was only 1 case. The other positions are educators and artists with 3 cases each.

Number of cases in violation of freedom of expression online



Sumber: Dokumentasi SAFEnet

From the aspect of articles, Article 27 paragraph 3 of the ITE Law (Defamation) is the most widely used with 10 cases. Followed by Article 28 paragraph 2 (Hate speeches) with 8 cases. The use of two articles at the same time appears too with Article 27 paragraph 1 (Pornography) with Article 27 paragraph 3 (3 cases). At last, the use of Article 27 paragraph 1 and Article 28 paragraph 2 with 1 case.



Number of cases collected by SAFEnet is indeed lower from the number of ITE Law cases that were recorded by the National Police. Data from the Directorate of Cyber Criminal Acts of the National Police, shows that number of investigations toward social media accounts always increase each year, from 1,338 in 2017, 2,552 cases in 2018, then soar high with 3,005 cases in 2019.

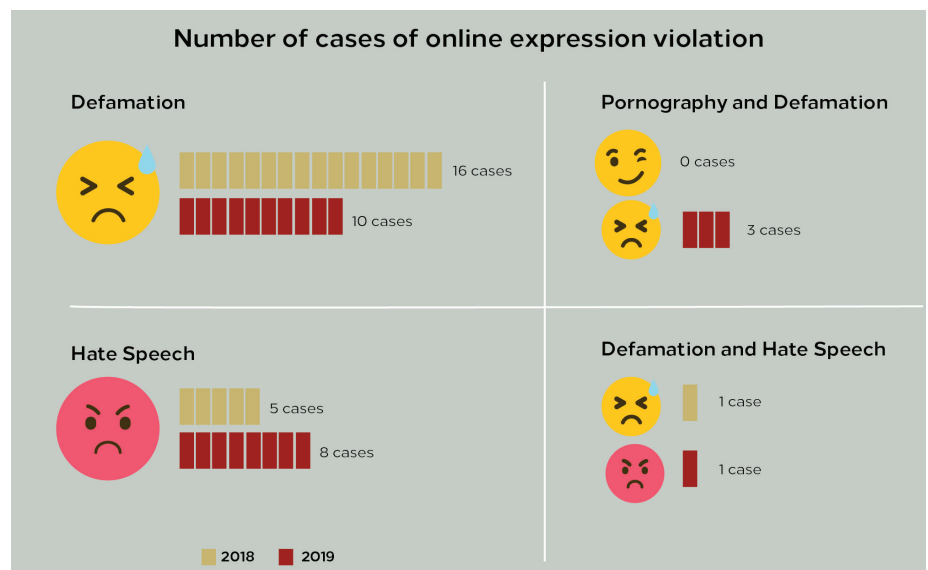
From the numbers, the most cases are investigations involving humiliation of public figures, authorities, and public institution. In 2017 there are 679 cases that were investigated involving humiliation, then rise to 1,177 in 2018 then decreased to 676 cases in 2019. The other high cases are the alleged provocation and hate speech. These 3 cases often refer to the use of article in the ITE Law.

Actors of criminalization

Public officials and politicians occupy the highest position as the actors criminalizing the right for freedom of expression online with 10 cases each. The number of public officials like police and state civil apparatus as the actors decreased from 11 cases reported in 2018. However, in 2019 there were many politicians acted as actors of criminalization; cases that were not found in 2018. Besides these two parties, the other actors were artists (3 cases), and professionals such as lecturers and doctors (2 cases).

From the regional distribution, cases of violation of freedom of expression online collected by SAFEnet are reported in 10 provinces. DKI Jakarta is the province with the highest cases (10 cases), then Southeast Sulawesi (3 cases), Aceh and East Java (2 cases each), and six other provinces with 1 case each.

The profile of criminal cases for the right for freedom of expression online in 2019 does not change much compared to the previous year. The dominant cases in 2018 involved journalist and media with 8 cases. Second place went to the general public with 4 cases. Civil apparatus was in third with 3 victims. Internet law also tangled educators (2 cases), activists and students each with a single case.



The presence of convictions throughout 2019 show that the right to freedom of expression online in Indonesia are not well protected yet. Articles in the ITE Law, especially Article 27 paragraphs 1 and 3 along with Article 28 paragraph 2 continue to be used to suppress freedom of expression that has been fought since 1998. Although freedom of expression is actually guaranteed in the Constitution and the Law on Human Rights.

The increasing trend in criminal prosecution of journalists and activists since 2018 is also a concern that threatens democracy.

The emergence of public officials and state apparatus as perpetrators of criminalization, shows that the ITE Law has increasingly been wrongly used to silence critical voices of public policy. Criminalization in the digital world is in line with the increasing repressive acts toward citizens who voiced their aspirations in the middle of the political year and afterwards.

As we all know in 2019, there was also a Legislative Elections (DPRD Regency/City, DPRD Province, DPR RI, and DPD) that was held along with presidential election simultaneously in all provinces. Two candidates that have competed since 2014, Joko Widodo and Prabowo Sibunto returned vis-a-vis for 190 million citizen votes.

Polarization due to public division which supported the two candidates since 2014, strengthened again in 2018 and peaked in 2019. Polarization at the grassroots was influenced by a digital political identity narrative battle by supporters of the two candidates that play through the religious and racial sentiments.

After the riots in May 2019, massive demonstration by the public happened in Jakarta, Yogyakarta, Palembang, Makassar and other areas on 24-26 September 2019. They refused the revision of the Corruption Eradication Commission (KPK) law and Draft of the Criminal Code (RKUHP). Protest were also voiced against the Land bill and Penitentiary Bill. Multiple bills were also deemed to deny the mandate of reform.¹ The police responded this action with repressive acts causing 3 deaths in Jakarta, while 2 Kendari students were shot death.²

Terror of the Country

The dynamical political situation related to the election, anti-corruption movement,

and action against racism also influenced the fulfillment of digital rights in Indonesia during 2019 and that, according to our projection, it will continue to be influential for years to come. By the end of 2020, SAFEnet published a projection that the situation of freedom of expression in Indonesia in 2019-2024 was on the status of Alert One. This projection is based on the increasing number of criminalization toward pro-democracy activists and journalists in 2018-2019.

This shows that the Reformation of 1998 is yet not enough to bring winds of change and protection to the works of press in Indonesia. Although press Law has been present, there is still the weakness of Press protection as it could be seen from the many occurrences of violence toward press both physically and non-physically. In addition to physical violence, actions such as the criminalization of journalists with the ITE Law, doxing to journalists, mobilization to destroy the media's credibility with online harassment on social media to the act of damaging reputation through one-star rating and bad review so that the media apps are removed from Google Playstore.

The arrest of several activists who carried out a combined actions and campaigns on public issues in social media was even more increasing and blatantly carried out, even though the available evidence did not meet the legal element. The terror by the country was shown with a number of arrests, like what happen to activist Ananda Badudu and film director Dandhy Laksono. Both were arrested even though police had not asked them as witness for information related to the alleged case prior to the arrest.

The hoax labeling of information posted by activists also becomes a new pattern before the criminalization occurs. The hoax labeling of the twitter post from human rights lawyer Veronica Koman was even carried out by the Ministry of Communication and Information and National Police. Several weeks later, Veronica became a suspect for allegedly sharing provocative content and false news. While the allegations of hoaxes against Dandhy Laksono posts were made by a number of buzzers. A few days later, Dandhy became a suspect of hate speech through a

¹ <https://nasional.kompas.com/read/2019/09/24/15440851/ramai-ramai-turun-ke-jalan-apa-yang-dituntut-mahasiswa>

² <https://www.bbc.com/indonesia/indonesia-50217875>

bizarre arrest procedure.

Those two cases are closely related to issue in Papua. What happened to Veronica Koman and Dandhy Laksono, shows that the country sponsors the repression for freedom of expression through online media against pro-democracy group that fight for justice for Papua.

Criminalization of Media and Journalist

Repression through digital media also continues to happen to journalists in 2019. Even though, freedom of the press in Indonesia has been guaranteed through Law No 40 Year 1999 about the press. To avoid criminal conviction of journalistic work, the Press Council and the National Police have also signed a Memorandum of Understanding in 2012. Broadly speaking, this memorandum of understanding contains the need for a press dispute to be resolved by the Press Council.

In fact, the conviction of journalists still happens by abusing several articles in the ITE Law, especially Article 27 paragraph 3 (defamation) and Article 28 paragraph 2.

First case happened to media Jawapos that was reported by football club Persebaya Manager to the Surabaya Police on 7 January 2019 related to the news titled "Green Force Pun Terseret". That news was actually the result of Jawa Pos Journalist investigation on the alleged soccer mafia when Persebaya competed with Kalteng Putra on 12 October 2017. Jawa Pos was reported with Article 310-311 KUHP and Article 27 paragraph 3 of ITE Law because it was considered to have slandered and ruined their good name. Even though, the news about Jawa Pos investigation is part of the press function in doing social control under protection of Article 3 of Law No. 40 Year 1999. Jawa Pos has been based on journalistic principles and carried it out for the public interest, so that it cannot be convicted with the article of the ITE Law and the Criminal Code.

Two Journalists in Kendari, Southeast Sulawesi, became the next victim. Fadli Aksar (Detiksultra.com) and Wiwid Abid

Abadi (okesultra.com) were reported by Andi Tendri Awaru, candidate for the National Mandate Party (PAN) Legislative Member of West Kendari-Kendari Electoral District, to Sultra regional police on 8 January 2019. That report happened after Fadli Aksar and Wiwid Abid Abadi Sultra published a news related to public report against Andi Tendri Awaru to Sultra regional police related criminal act allegations of faking residence certificate and administration. After demonstrated by the local journalists group, Sultra regional police finally pushing the case to be resolved by the Press Council.

Still in Southeast Sulawesi, Liputanpersada.com reporter in Central Buton District, Mohammad Sadli Saleh, was taken into custody after highlighting road construction from the regional budget (APBD). He was reported by the Head of Legal Section of the Central Buton District Government, Akhmad Sabir and the Head of the Information and Communication Office of Buteng, La Ota with Article 27 paragraph 3 of the ITE Law (Defamation), Article 28 paragraph 2 of the ITE Law (Hatred).

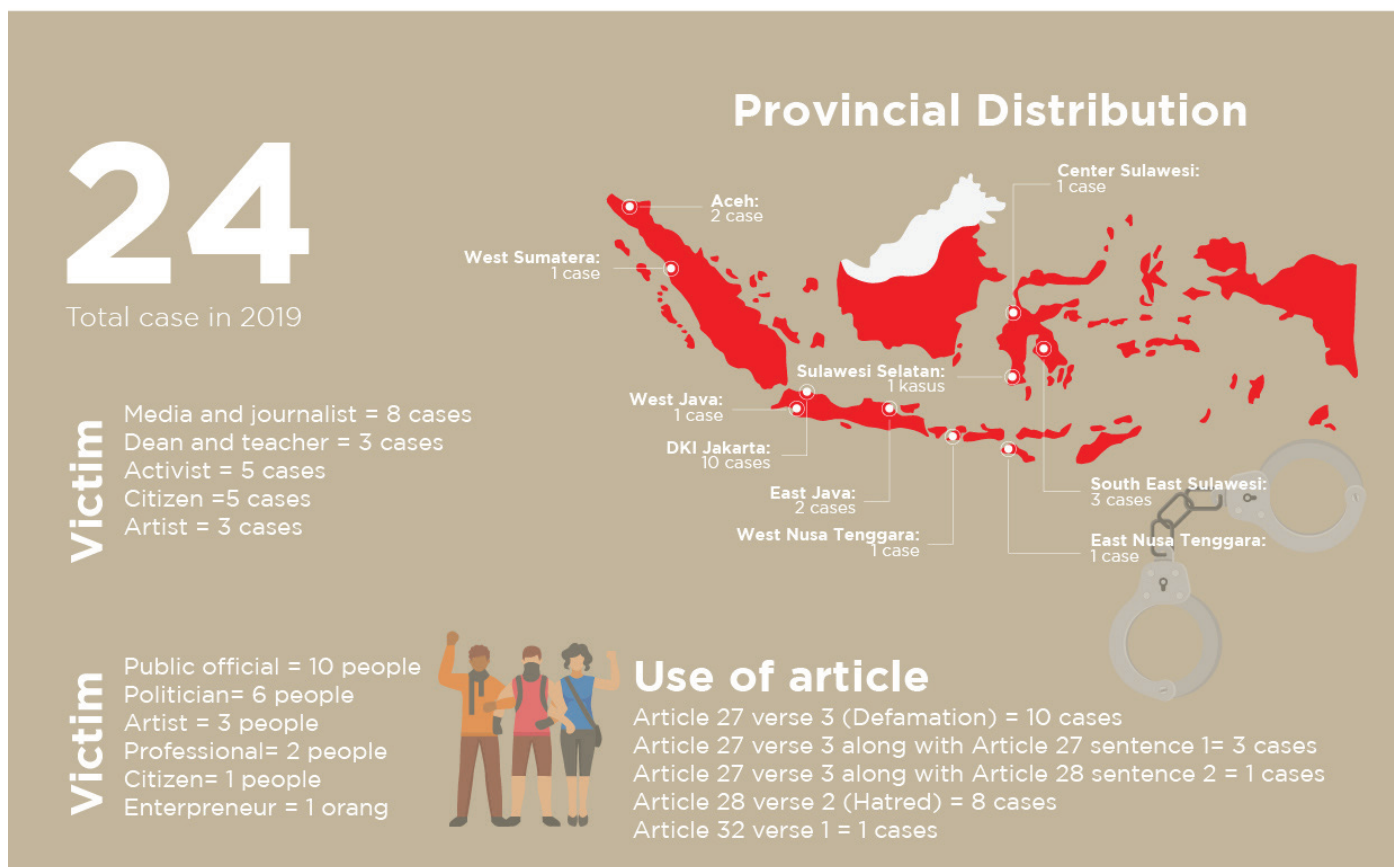
Central Buton Police ignored the Memorandum of Understanding between the National Police-Press Council in processing this case to court. As same as with the police, on 26 March 2020, PN Pasarwajo panel of judges sentenced Sadli to 2 years in prison.

Beside journalistic work, criminalization happens too toward information content that were delivered by journalists on social media. This happened to journalist and documenter film director Watchdoc, Dandhy Laksono on 23 September 2019. Dandhy was arrested at his home after uploading two photos and several news articles online, as follow:

"JAYAPURA (photo 1). Papuan students who take exodus from campuses in Indonesia, open a post at Cendrawasih University. The officials transporting them from campus to Expo Waena. Riot. Someone died."

"WAMENA (photo 2). High school students protest the racist attitude of teachers. Faced by the authorities. The city riots. Many have gunshot wounds," he continued. "

Criminalization Data on the Right to Freedom of Expression



Infographic: Criminalization Data on the Right to Freedom of Expression

Dandhy was charged with Article 28 paragraph (2) Article 45A (paragraph 2) of the ITE Law about Hate. However, before Dandhy was arrested, the information shared by Dandhy Laksono was bombarded with many hate comments and even labeled as a hoax, even though the information that Dandhy uploaded are based on several credible media reports.

The arrest of Dandhy was also arbitrary. He was arrested at his home in Bekasi, West Java then escorted to Jakarta Metro Jaya Police on Thursday 26 September 2019. The arrest was carried during rest hour, that is 23.00 WIB, without an arrest warrant. Dandhy was released as a suspect, after an inspection for around 7 hours. Another irregularity was that Dandhy was arrested based on the report of a police.³

Criminalization of Activists

Not only journalists, the cases of silencing freedom of expression also happened to activists. The first case was experienced by Fransiskus Olarugi Lamanepa or commonly known as Frank Lamanepa, an activist of the East Flores United People Coalition (KRBF).

He was named a suspect by investigators from the East Flores Police (Flotim) after criticizing Flotim Regional Secretary Paulus Igo Geroda, who at that time was concurrently the Head of the Flotim Regional Bendana Management Agency (BPBD). His writing in the form of a poll on the Suara Flotim Facebook group was reported to the Flotim Police by the Regional Secretary of Flotim on 10 June 2019 for allegedly containing defamation.

Frank was found guilty, after the trial of the Preliminary Decision on Lawsuit against the Flotim Police was rejected by the Judge.

³ <https://tirto.id/kasus-dandhy-laksono-ananda-badudu-lampu-kuning-untuk-demokrasi-eiUl>

Meanwhile, the second case of criminalization of activists related to freedom of expression happened to Emerson Yuntho, who is also former Indonesian Corruption Watch (ICW) activist.

He was reported by the former chairman of the DPR RI, Setya Novanto to the West Java Regional Police regarding his comments on Twitter. In his tweet, Emerson questioned the whereabouts of Setya Novanto, who was serving a sentence at the Sukamiskin prison, Bandung, West Java. Emerson was then reported with Article 45 paragraph (3) in conjunction with Article 27 paragraph (3) of Law of the Republic of Indonesia No. 19 of 2016 concerning amendments to RI Law No 11 of 2006 concerning ITE.

Musician and activist Ananda Badudu was arrested for raising funds through KitaBisa for student demonstrations against the RKUHP and the KPK Law in front of the DPR / MPR Building on Tuesday 24–25 September 2019. The arrest of Ananda Badudu only took place one day after Dandhy Laksono and was carried out arbitrarily. Ananda's boarding house in Tebet Barat, South Jakarta was banged on while she was asleep. He was then taken to the Metro Jaya Police on Friday 27 September 2019 at around 04:25 WIB.

Similar criminalization has also occurred for activists who are vocal in voicing the issue of Papua. After journalist Dandhy Laksono, human rights lawyer for Papua, Veronica Koman was named a suspect by the Head of the Regional Police of East Java on 4 September 2019. Veronica was suspected of provoking and spreading fake news on her social media.

There are three contents of Veronica's tweets which are accused of being provocative and hoaxes related to the racism incident at the Papua Student Dormitory in Surabaya, on 16 August 2019. The first content is: calls for the mobilization of monkey action to take to the streets for tomorrow in Jayapura (18 August 2019). The second content: the moment the police shot into the Papuan dormitory, a total of 23 shots including tear gas, the children did not eat for 24 hours, thirsty, locked up, told to go out into the sea of masses. And the third content: 43 Papuan students were

arrested for no apparent reason; 5 people were injured and 1 was hit by tear gas shot.

Veronica Koman was charged with four laws at once, namely the ITE Law, 160 Criminal Code Law, Law No.1 of 1946 concerning Criminal Law Regulations, and Law 40 of 2008, concerning the Elimination of Racial and Ethnic Discrimination. On 20 September 2020, Veronica Koman was listed on the People Wanted List (DPO).

Hoax labeling on Veronica Koman and Dandhy Laksono has become a new pattern of cyber-attacks on critical groups. Before the determination of the suspect by the East Java Regional Police, the Ministry of Communication and Information Technology first labeled Veronica Koman's tweet a hoax with an article dated 19 August 2019 entitled [Hoaks] Surabaya Police Kidnapped Two Food Deliverers for Papuan Students “.












In fact, Veronica Koman herself did not write the word “kidnap” in her tweet on Twitter. Veronica Koman's original tweet read: “2 people who deliver food and drink for dormitory residents who have not eaten or drunk since noon have just been arrested by the police”. After criticism of the hoax labeling with content manipulation, Kominformo clarified and withdrew the article.

Criminalization of Academics

2019 also marks the rampant criminalization of academics, as happened to Syiah Kuala University lecturer Saiful Mahdi and University of Indonesia lecturer Ade Armando.

Saiful Mahdi was reported to the police by the Syiah Kuala University's Dean of the Faculty of Engineering, Taufik Saidi, on charges of defamation, after he gave a statement in the WhatsApp Group (WAG) of UnsyiahKita and WAG for Research and Development Center regarding the irregularities in the process of admitting Candidates for Civil Servants (CPNS) at the Faculty of Engineering in March 2019.

On 30 August 2019, Saiful Mahdi received a summon as a suspect in the case of

Instagram		534 cases
WhatsApp		431 cases
Facebook		304 cases
Telepon/ SMS		198 cases
Twitter		80 cases
Lainnya		70 cases
Line		55 cases
Blogpost		32 cases
Marketplace		30 cases
Email		20 cases
Telegram		9 cases

Prior to that report, Ade Armando's post went viral and sparked harassment. On social media, the hashtag #tangkapAdeArmando echoed and had become a trending on Twitter.

However, data of cases that are collected by SAFEnet is only the tip of the iceberg. The real data could be 10 times higher. As comparison is the data from the Police that could be accessed by the public in the Cyber Patrol website. According to the website, internet-related cases in 2019 reached 4,586 cases. Cases related to spreading provocative content are the most dominant with 1,769 cases. Referring to the cases handled by SAFEnet so far, provocative accusations are often inadequate and could be interpreted in many ways.

From the platform side, the media that mostly used by the accused crime perpetrators related to the Internet are as follows:

Other data that could be taken as reference are total cases related to the ITE Law as documented at the Supreme Court (MA) website. With the keyword "UU ITE" that were registered along 2019 result 212 cases. But we realize that further investigation is needed whether all these cases are purely related to defamation of a multi-interpretation nature and carried out as part of criticism or not.

defamation using electronic means as referred to Article 27 paragraph (3) of the ITE Law. After undergoing the first trial on 17 December 2019, Saiful Mahdi was sentenced to 3 months in prison and a fine of Rp.10,000,000, a subsidiary of 1 month in prison by the Banda Aceh District Court Judges.

Meanwhile, the criminalization against Ade Armando is related to political issues. He was reported by DPD RI politician Fahira Idris regarding the meme of DKI Jakarta Governor Anies Baswedan with a joker face with the words "Bad Governor Starting from a Dismissed Minister" on 31 October 2020. Fahira reported that Ade used Article 32 paragraph 1 of the ITE Law concerning the prohibition of changing the form of electronic documents and or electronic information.



Journalist Safety Committee

On 5 April 2019, SAFEnet together with nine other organizations joined the Komite Keselamatan Jurnalis or Journalist Safety Committee (KKJ), a coalition initiated by the press community as a form of collaboration to handle cases of violence against the press and journalists. This initiative also emerged as anticipation of the increasing trend of violence against journalists in the political year.

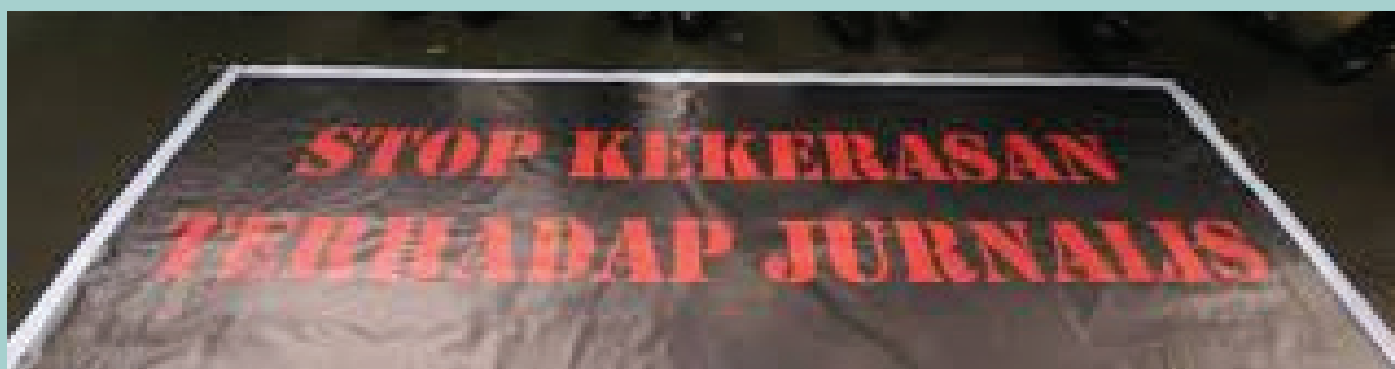
The Committee has developed Standard Operating Procedures (SOPs) which will serve as guidelines in the handling and preventing cases of violence toward journalists and media workers so that they do not happen again.

In this coalition, SAFEnet has a role to assist the campaign and participate in advocating

for cases of criminalization of journalists who use the catchall articles of the ITE Law. In addition, SAFEnet filled the advocacy void in cases of criminalization of journalists due to their personal views and opinions.

The KKJ cannot handle this case directly because of the existence of SOPs that limit advocacy space only to cases related to journalistic work and products.

In addition to assisting and providing legal assistance, the KKJ also verifies cases for each case of violence that occurs to journalists. As well as opening the Anti-violence hotline service for journalists who experience violence at numbers 0812-4882-231.





RIGHT TO FEEL SECURE

In 2019, Indonesia as the country with the fifth highest number of internet users in the world planned to issue its first law on cybersecurity. Through the Bill on “Cyber Security and Resilience”—the name of the regulation proposed by the DPR Legislative Body, Indonesia will become the newest Southeast Asian country which has cyber security laws following Singapore, Thailand and Malaysia.

This desire is understandable considering that Indonesia needs this cyber security law to protect its more than 150 million Internet users. These users were vulnerable to at least 232.45 million cyber-attacks in 2018 and 205 million cyber-attacks in 2017. At least in May 2019 alone, there were 1.9 million cyber-attacks recorded. It is estimated that these cyber-attacks could result in a loss of IDR 478.8 trillion (US \$ 33.7 billion). The loss figure is equal to almost one-fifth of Indonesia’s 2020 state budget.

One of the most frequent cyber-attacks is malicious software (malware), software that damages computers and endangers the

security and confidentiality of information. Malware can be in the forms of trojan viruses, worms, ransomware, spyware, scareware, and adware.

Referring to the results of the latest research by Microsoft Security Endpoint Threat Report 2019, malware attacks in Indonesia rank the highest in the Asia Pacific region, namely 10.68% in 2019. This figure is twice the regional average. Indonesia is also registered as having the second highest ransomware case rate in the entire Asia Pacific region, namely 0.14%. This is still 2.8 times higher than the regional average. Meanwhile, Indonesia’s cryptocurrency mining case rate stood at 0.10% in 2019, two-times higher than regional and global averages, and the 4th highest case rate across the region.

Apart from malware attacks, Indonesia also has frequent personal data theft. On 12 August 2019, there was a massive data theft of at least 35 million customers of Lion Air and its subsidiaries, including Thai Lion Air in Thailand, Malindo Air in Malaysia, and Indonesia-based Batik Air. Also, the stolen

personal data is sold online, including full name, date of birth, telephone number, email address, passport number, passport expiration date, and other details. From Indonesia, there were 156,000 consumer data that were stolen.

An internal investigation by Malindo Air via a cybersecurity firm revealed that the perpetrators were two former employees of e-commerce service provider GoQuo (M) Sdn Bhd at their development center in India accessing and stealing Lion Group customer data. Even though the culprit was caught, the biggest data leak incident from Asia-Pacific is already circulating on the online black market.

Another incident occurred on 13 December 2019 when the Ministry of Home Affairs' Directorate General of Dukcapil and the private company VeriJelas had signed a cooperation agreement (PKS) related to rights to access data verification of electronic Identity Number (KTP-el) and biometrics for KYC (know-your-customer) services. SAFEnet highlighted this collaboration, especially because the Directorate General of Dukcapil had previously collaborated with Astra, as well as more than 1,300 institutions that were invited to cooperate in using the data. In utilizing this data, the Dukcapil should first inform the data owner that a third party will have access to the Identity Identification Number (electronic KTP) and biometric data. If there is no approval from the data owner, it is suspected that there has been a violation on the right to privacy.

Cyber-attacks and data theft should be prevented by the existence of cybersecurity regulations and protection of personal data. However, unfortunately, the formulation of the Bill on Cyber Security and Resilience proposed in 2019 actually poses a serious threat to citizens' freedom of speech and will create a super body institution that will be above law enforcement agencies. The law will arm the country in the fight against cyber threats. It will designate the BSSN as the implementing body to coordinate with the armed forces, police, the attorney general's office, intelligence agencies and other government ministries and agencies.

Moreover, in its formulation and discussion, there is no multi-stakeholder involvement in the drafting process of this Cyber Security Bill, there are no discussions with other government agencies, there are no dialogues with the private sector related to cybersecurity or e-commerce, even not asking for input from civil society organizations. That is why SAFEnet spoke to the public and asked the Indonesian legislature to repeal the authoritarian cybersecurity law, and the DPR legislature finally withdrew the Cyber Security and Resilience Bill in September 2019.

In addition, in Southeast Asia, personal data protection laws only exist in a few countries, while in Indonesia, there is no Personal Data Protection Law (PDP Law). The absence of this law poses a challenge when data breaches occur at the regional level. While different countries have different mechanisms for dealing with data protection, the treatment of affected individuals is inconsistent. This can lead to discrimination. This incident is a good example for highlighting the regional inability to address data protection.

Other things that need to be highlighted in digital security in Indonesia are cyber threats and cyber-attacks against women and communities at risk, such as journalists, anti-corruption activists, environmental activists, human rights defenders, LGBTIQ people, and religious minorities. Apart from physical attacks, they experienced digital attacks in the form of doxing, DDoS attacks on media outlets, unlawful wiretapping, account hacks and instant messaging.

Vulnerable Bodies in the Digital World

Currently, visible assets are transformed into digital entities such as usernames, IP addresses, telephone numbers, e-mail addresses, photos, texts, videos, and various information which are unique in digital spaces. Not only continues to increase in number, vulnerable assets in the digital world also face various threats facilitated by digital media.

The Digital At-Risks (DARK) sub-division under SAFEnet's Right to Security Division noted that vulnerable bodies in the digital world are those with the identity of children, women, LGBTQ (lesbian, gay, bisexual, transgender and queer), journalists, activists (human rights issues, anti-corruption, the environment, religious minorities, and whistleblowers). During 2019, DARK noted various gender-based cyber violence (GBVO) which we previously referred to as online gender-based violence (GBVO) with findings will be elaborated in the next sections.

Spread of Intimate Content Rampant

KBGS is an act that makes someone insecure or feeling insecure; attacks or any acts that have a greater impact on one's gender or sexuality, which occurs when they are connected to the Internet or facilitated by digital technology. Usually this form of violence stems from violating privacy and / or committing non-consensual actions to one or many individuals at once.

Throughout 2019, SAFEnet received 60 GBVO case complaints. A total of 44 case complaints were referred by Komnas Perempuan to SAFEnet, which has been Komnas Perempuan's official referral partner since July 2019. The other 16 complaints came from various SAFEnet communication channels, including those directed by partners or other communities to make their complaints reported to SAFEnet.

Of them, 53 victims who complained were women and 7 others did not identify their gender. The most reported forms

of GBVO are the distribution of intimate content without consent (nonconsensual dissemination of intimate images or NCII) with 45 cases, violations of privacy (such as doxing, non-consensual surveillance, wiretapping, unauthorized access) with 7 cases, creation of copycat accounts (impersonation) with 2 cases, showing off the genitals in a non-consensual digital space (digital exhibitionism) with 3 cases, and other forms of KBGS such as acts of shaming victims in public digital spaces (online shaming) or violations of the victim's privacy outside of the categories above.

This figure certainly does not represent the overall number of KBGS incidents in Indonesia. Komnas Perempuan's 2020 Annual Report entitled "Increased Violence: The Policy on the Elimination of Sexual Violence to Build Safe Spaces for Women and Girls" states that there are at least 281 cases in 2019, an increase of 300% from 97 cases in the previous year. The form of threat of spreading pornographic photo content was the most frequently reported and reached 91 cases.

From 45 complaints of NCII cases, SAFEnet found 22 of them were sextortion, or threats of non-consensual distribution of intimate content accompanied by extortion in the form of requests for money or more intimate content. There were also 12 cases of revenge porn or threats to spread intimate content by couples who did not want to break up or separate or ex-partners who forced them to reconnect. In addition, 11 other NCII cases did not have the above motive or at the time of the complaint and during the consultation this motive had not yet been seen.

The majority of victims who were threatened or had experienced GBVO in the form of distribution of intimate content were aged 18-25 years, especially those who faced sextortion (14 people). This can be influenced by several things, such as the age range of 18-25 years old where the penetration of

Complaints on KBGO Cases handled by SAFEnet (n=60)

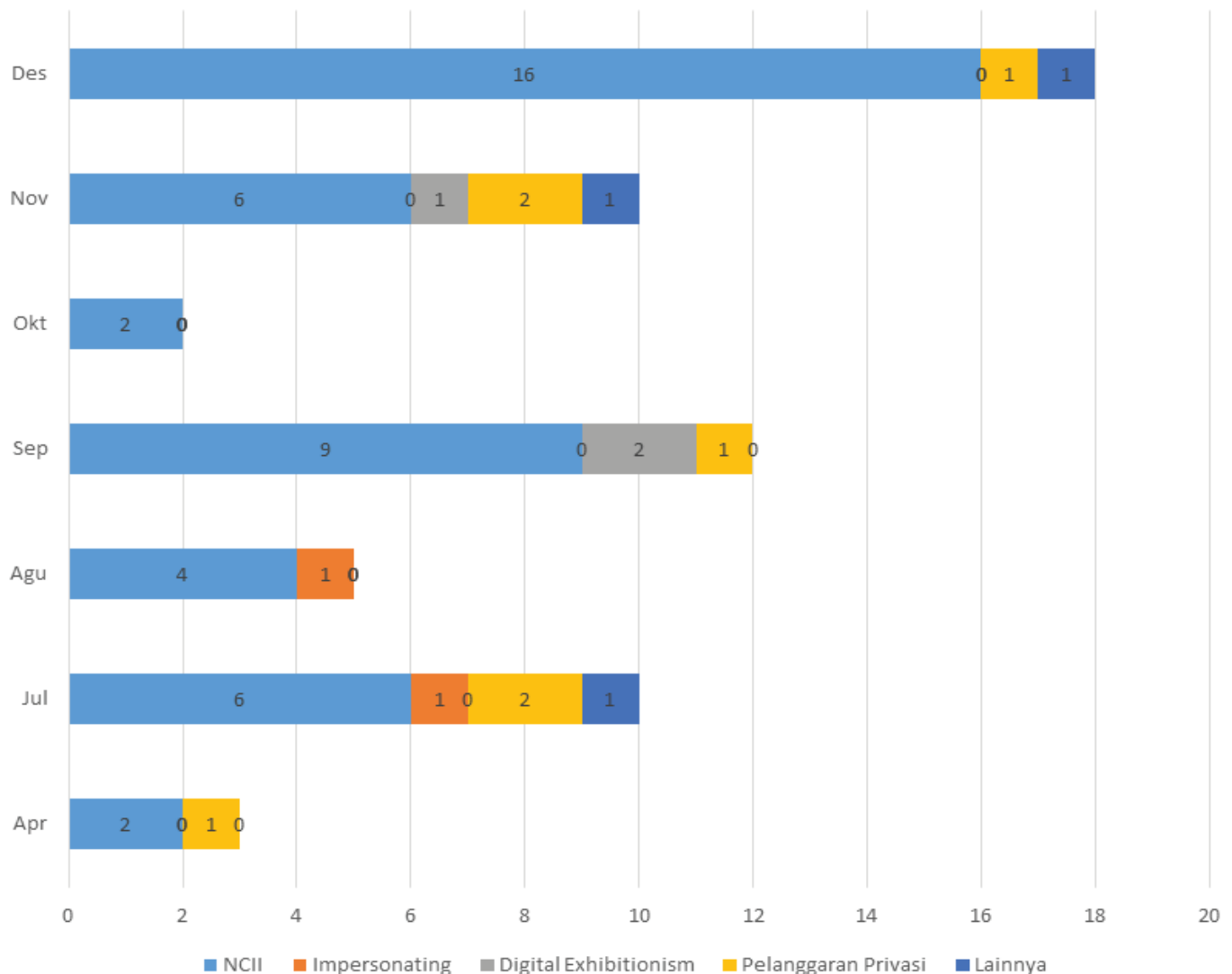


Table 1 KBGS complaints that came to SAFEnet

* 2012-2018 data based on SAFEnet 2018 Annual Report "The Path to Fight for Digital Rights"

the Internet is the highest,¹ they can access assistance or report their cases to agencies, such as Komnas Perempuan. There were 36 out of 44 complaints related to NCII referred from Komnas Perempuan to SAFEnet.

Regarding the threat of spreading intimate content, two of the complaints that came in

had an impact on the victim's work as activists, both of whom were deliberately attacked to delegitimize their activism. A² faced GBVO because the perpetrator had personal motives and had manipulated the victim to build unequal romantic relationships, so A experienced NCII which was categorized as revenge porn. A's intimate content was used by the perpetrator as a tool to intimidate A and was also threatened to be shared in A's

¹ The 2018 Indonesian Internet User's Penetration Survey and Behavioral Profile by the Indonesian Internet Providers Association (APJII) accessed on 18 May 2019 stated that based on the penetration rate, the highest age range for internet users in 2018 was 15-19 years (91%), 20-24 years (88.5%), and 25-29 years (82.7%).

² Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

Age of Victims Experiencing KBGO in Form of NCII (n=45)

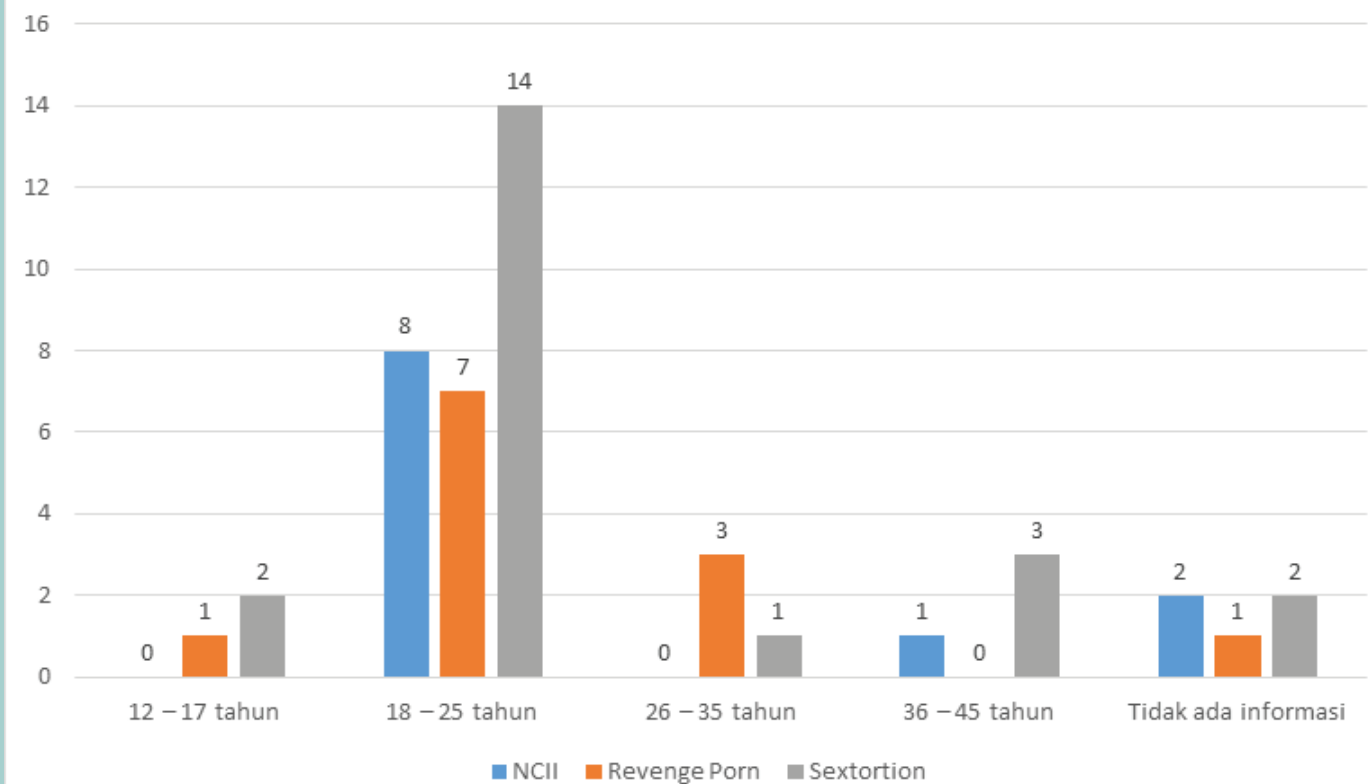


Table 2 Number of Complaints for KBGS Cases Assisted by SAFEnet per month during 2019.

work spaces to destroy his reputation and credibility.

In contrast to A's experience, B³ is an activist who has had political-motivated GBVO. The main culprit is unknown, but a bunch of unclear accounts appeared on social media, such as Facebook, Twitter, and Instagram, moving like a buzzer deliberately distributing nude photos of B stolen from the victim's hacked cellphone, then manipulated with compositions showing B's naked body juxtaposed with work partners, who are also activists, with slanderous affairs to delegitimize their voices as activists who were advocating the issue of revision of the KPK Law at that time.

SAFEnet's observations in receiving and accompanying incoming complaints also show several things, namely that the violence experienced by victims may not be in one form as indicated by the statistics

above. Victims often experience several forms of GBVO at once, such as doxing or dissemination of the victim's personal data, such as full name, cellphone number, or personal account, without consent to cyberspace.

The complaint from C⁴, for example, said that the perpetrator carried out surveillance on him using digital technology in the form of installing a smart phone application that has a feature that can find out the location of the victim in real-time on the victim's cellphone (spyware). The victim also faced phishing attempts⁵ in the form of link manipulation⁶ by the perpetrator who wanted to hack into the victim's social media account, but this attempt was thwarted.

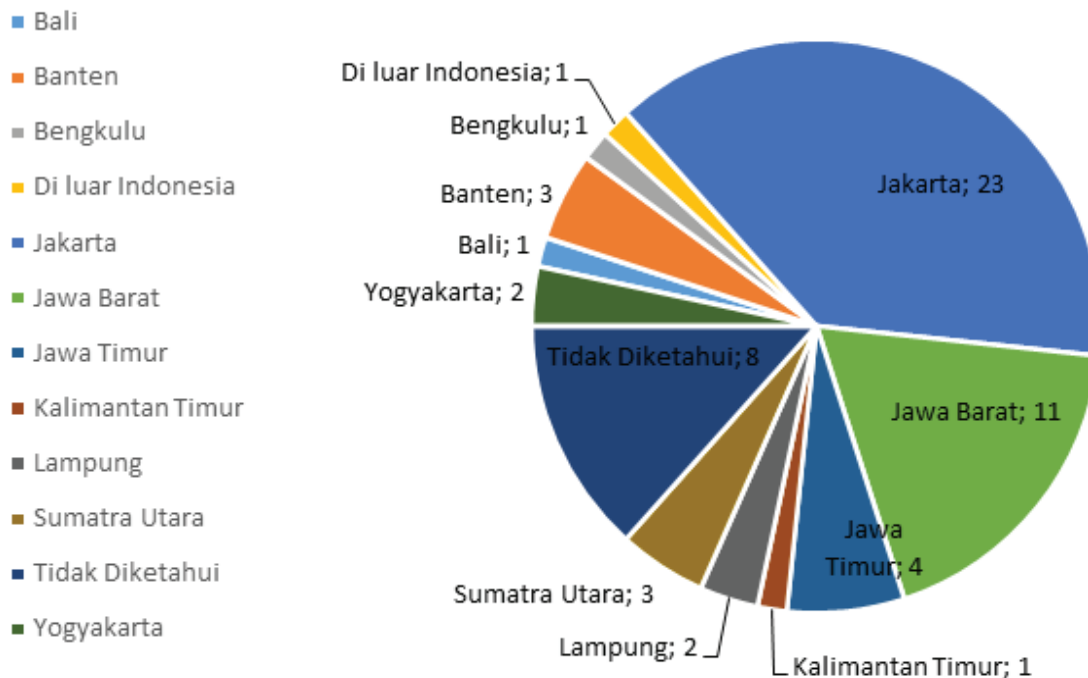
4 Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

5 Phishing is a form of cyber crime when the perpetrator deliberately pretends to be or creates a legal or trusted identity to lure the victim to provide personal data information, which will usually be used to support other cyber crimes against the victim, such as hacking, account takeover, and so on.

6 Link manipulation is a phishing act by sending a link whose website appearance is made similar to a website that is familiar to the victim, usually accompanied by a form or column to enter personal data, such as names, keywords, and others.

3 Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims..

Domicile of KBGO Victims Handled by SAFEnet(n=60)



Tabel 3 Age of NCII-form KBGS victims who were accompanied by SAFEnet in 2019

In NCII cases, the perpetrator often took advantage of the victim's psychological situation who did not want the violence they experienced to be known by others, especially those closest to the victim such as parents and family. The perpetrators intimidate the victims to comply with the perpetrators' wishes or requests. The victim's psychological situation is also sometimes used by the perpetrator to obtain personal information about the victim, as experienced by C. The victim's vulnerability also increases when the GBVO that she experiences is related to LGB (lesbian, gay and bisexual) sexual orientation, which in Indonesia has often been subject of discrimination. At least two cases handled by SAFEnet involved LGB sexual orientation.

SAFEnet also found that the violence was cross-digital and multiplatform. The perpetrators used various digital technologies to communicate with the victim, from dating apps to chat apps, such as WhatsApp, Line; application correspondence (e-mail); or take

advantage of the direct message feature on social media or even an entertainment application that doubles as social media, such as Hago.

As long as these digital platforms have interactive features between users, then it has the potential to become a space for digital violence.

The use of various digital communication technologies allows victims and perpetrators to be in different locations, such as different cities, different provinces, even different countries. In SAFEnet's records, there were 2 KBGS complaints experienced by victims who were Indonesian citizens and were abroad during the occurrence of the violence. One of them was with the perpetrator being in Indonesia, and the other with the perpetrator who claims to be a foreigner and persuades the victim to go abroad to meet him.

The variety of situations faced by victims and their needs makes the steps and actions

taken not based on a single solution but on the results of risk mapping. During the mentoring and consultation process with GBVO victims and survivors, SAFEnet took action in the form of one or a combined steps: by providing advice on digital security (58%), only recording cases because the communication did not continue (35%), helping to improve the digital security of victims (30%), assisting the reporting process to digital platforms (17%), connecting with LBH (13%) and other assisting agencies (17%), contacting the perpetrator to seek mediation (5%), assisting the reporting process to the police (3%), and provide legal advice (3%).

When accompanying complaints on GBVO cases throughout 2019, SAFEnet also conducted face-to-face consultations with victims (23%). However, the majority of mentoring is done online because the victims' domiciles are in various places.

Not all recorded complaints result in reporting to the police, because victims choose not to do so. The reasons include they were not wanting to be caught by parents, the long timing of process, fear of victim blaming or being criminalized by the ITE Law, fees, and others. From cases accompanied by SAFEnet to the reporting stage to the police, it is carried out in coordination with legal aid agencies, such as LBH APIK Jakarta, LBH Jakarta, and LBH Bandung.

Machines and Algorithms are also Doers

One of the interesting case complaints that came in to SAFEnet is an unintentional privacy violation by a system that does not understand the perspective and impact on the victims. In D's case, D⁷ experienced KBGS because D's name as a victim of sexual violence was not disguised in court decisions and the name appeared in Google search results. The impact was that D experienced the stigma that victims of sexual violence often experienced.

This case shows the characteristics of KBGS are not always related to direct sexual violence, but also in the digital footprint that comes after. In this case, a court decision that did not disguise D's name was uploaded to the Supreme Court's website in digital format (pdf) and appeared on Google's search engine result when the victim's name is typed.

This case also shows that although almost all KBGS cases always occur on digital platforms that provide direct and two-way interactive features between platform users, KBGS can still occur even when the digital platform does not allow direct interaction between users, such as the Google search engine. This happens because the interaction between the user and the algorithm. The perpetrator may not only be human, but incidentally also in the form of digital technology, namely a search engine algorithm system and an institution's website.

In this case, it is regrettable that the court's decision file has ignored the Supreme Court Decree Number 1-144/KMA/SK/I/2011 concerning Guidelines for Court Information Services. In the Decree's Point VI concerning Procedures for the Disclosure of Certain Partial Information states that in regards to the Information That Must Be Announced and Information That Can Be Accessible to the Public, it is stated that the Information Officer is obliged to obscure the case number and identity of the victim and witness in several cases, including criminal acts of decency.

On the other hand, this is a part of gender-based violence itself due to the stigma in society that judges victims of sexual violence, so that the impact of this incident creates new violence and trauma to the victim, in addition to repeating old trauma.

Another interesting thing about this case is the allusion to the ITE Law No. 19/2016 Article 26 Paragraph 3 regarding the right to be forgotten and Government Regulation No. 71/2019 concerning Implementation of Electronic Transactions and Systems (PSTE). Article 15 Paragraph 2 is related to the right to erasure and exclusion from the list of search engines (right to delisting).

⁷ Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

Efforts to take legal action in this case have not made use of the above regulations based on the victim's decision. However, it would be interesting to note that these articles are used to answer the needs of victims of GBVO, who often experience repeated violence because content that is a digital trail of violence experienced by victims is still circulating in digital spaces on various platforms, both in nature public or limited in groups, instead of being a regulation that is used for interests that are detrimental to the public, such as efforts to erase traces of corruption.

Pseudo Justice in the Realm of Law for Victims

When it comes to seeking legal justice, the existence of Article 27 Paragraph 1 of the ITE Law regarding content that violates decency and the Pornography Law often criminalizes or intimidates GBVO victims related to the threat of content or sexual dissemination, so that many choose to have no legal domain. Instead of feeling protected, victims are afraid that they won't be protected. In addition, the legal process is long and drains energy, as well as money, are also the reason for the victim not to report to the police.

Everyone knowingly and without rights distributes and / or transmits and / or makes electronic information accessible and / or electronic documents that have content that violates decency. - Article 27 Paragraph 1 of the ITE Law

One of the cases that posed an emergency situation in handling the GBVO is the Baiq Nuril Maknun⁸ case which has received great attention from the public since 2018, because of justice that has not been obtained even though it has faced legal proceedings since 17 March 2015. Attention and public pressure have indeed been later resulted in the granting of an amnesty by the President of the Republic of Indonesia Joko Widodo on 29 July 2019 and freeing Nuril from the threat

of imprisonment for 6 (six) months and a fine of Rp. 500 million, a subsidiary of 3 months in prison.

Many things were shown from the resolution of Nuril's case, especially the stuttering of legal instruments with the context and perspective that Nuril faced as a victim of verbal sexual harassment by her own superior. This can be seen from the Supreme Court's issuance on Decision Number 574 / Pid.Sus / 2018 at the Cassation level and handed down a sentence on her, and then also rejected Nuril's Reconsideration Request as a Convict based on the Supreme Court Decision Number 83 PK / Pid.Sus / 2019 in Review level on 4 July 2019. Komnas Perempuan regrets these decisions for not heeding Supreme Court Regulation No. 3/2017 concerning Guidelines for Adjudicating Cases of Women Facing the Law.⁹

Another disappointment, in an attempt to request a judicial review (PK) to the Supreme Court which requires new evidence (novum), Nuril sued the perpetrator to the West Nusa Tenggara Regional Police with the Criminal Code Article 294 Paragraph 2 point 1 concerning Obscene Acts in a Work Relationship with number report: LP / 334 / XI / 2018 / NTB / SPKT, yet she had to see bad result. The report was discontinued on 28 January, because it was deemed to have insufficient evidence and no physical contact had occurred. It proves that the legal umbrella in Indonesia is still unable to provide justice for victims of sexual violence, especially those who do not have evidence of physical contact.

Apart from Nuril, in 2019 there were two GBVO cases that were also advocated by SAFEnet together with various partners that resulted in court decisions, namely the E¹⁰ and Kennedy Jennifer Dhillon¹¹ cases. These two cases show the same as the Nuril case,

⁸ We have received approval from Baiq Nuril Maknun for the inclusion of his name in this report.

⁹ Amalia, S. (2019, Juli 10). Komnas Perempuan: Supreme Court Should Use PERMA on Women's Case for Baiq Nuril. Accessed from Magdalene: <https://magdalene.co/story/kasus-baiq-nuril-seharusnya-didasarkan-perma> pada 16 Juni 2020

¹⁰ Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

¹¹ We have received approval from Kennedy Jennifer Dhillon for the inclusion of his name in this report.

that it takes a big effort and a long journey to demand justice for the KBGS that they have experienced.

The legal process that E experienced was similar to what was experienced by Nuril in terms of time. If Nuril had to go through a legal process of about 4 years and 4 months, E experienced it for 5 years. E was reported in early 2014, and had experienced a prison term of 8 days in the end of 2014, before being found guilty at the Bandung District Court. E received acquittal when E appealed to the High Court, although E later faced a cassation verdict which found her guilty. E was finally acquitted in a judicial review by the Supreme Court in January 2019.

E is a housewife who was caught in the ITE Law case on her husband's (now ex) report. This case started with E, who had experienced Domestic Violence (KDRT) by her husband since 1994 and only dared to report it to the police in 2013. Her husband responded to this report in 2014 with a report to the police with evidence of a conversation in E's Facebook inbox with his friend who is suspected of having committed immoral acts and violating the ITE Law Article 27 Paragraph 1.

In this case, E's husband committed a privacy violation by accessing E's Facebook account secretly to take a screenshot of the conversation, print it, and duplicate it as evidence of reporting. The facts at the trial found this to be untrue. Based on the Minutes of the Forensic Examination Results from Bareskrim Polri, Directorate of Economic and Special Crimes presented at the trial in early March 2015, it was stated that the evidence printed by the perpetrator was not found on E's Facebook, or the evidence submitted by the perpetrator did not show any immoral acts as alleged.

For 4 years 11 months, E went through the legal process to be free from accusations of not being proven by perpetrator of domestic violence which was accommodated by the use of the catchall article of the ITE Law

Article 27 Paragraph 1 and the presentation of screenshot evidence of conversations that had violated E's privacy by breaking into his Facebook account.

Kennedy had a different story from Nuril and E. As a victim of GBVO, legal justice was present for her case, but not without her hard struggle during the process. There are various efforts made by Kennedy to seek justice for the KBGS experienced, namely the distribution of private cellphone numbers with fake identities on various online dating applications such as BeeTalk, WeChat, Badoo, and others.

Kennedy's personal number was posted on the digital platform accounts as an account that offers massage and spa services as well as sexual services. These accounts do not contain real or full names, or contain photos of Kennedy, but rather sexy photos of someone else which were stolen from Facebook and Google. As a result, Kennedy received many text messages and video calls on WhatsApp and her cellphone from men who contacted him to ask about the services mentioned in these digital accounts.

This disturbance did not only happen to Kennedy. It is known that the perpetrator also carried out a similar KBGS act on at least 4 other victims with a motive of different political views regarding the 2017 Jakarta Regional Election candidates.

"I hope that state institutions can also upgrade themselves to be smarter in seeing the reported cases so that it is no longer my job as a victim to find the perpetrators, look for evidence, and look for signs of the perpetrators."

This call was made by Kennedy at the press conference "Gender Based Violence Online (GBVO): Understanding and Protecting Women and Vulnerable Groups"¹² held by SAFEnet. During the legal process, Kennedy had to struggle to obtain various information

¹² The live broadcast of this press conference can be watched on Youtube via a link [s.id/YTliveGBVO](https://www.youtube.com/watch?v=s.id/YTliveGBVO)

to be used as evidence and to seek clues about the perpetrators, which should be part of the police's duties in investigations. Kennedy took the initiative to contact the digital platforms BeeTalk, WeChat, and Badoo, which contained fake accounts selling massage and prostitution services created by the perpetrator. She also sent an e-mail to the Ministry of Communication and Information to take action on these applications.

Kennedy's persistence in guarding her own case and continuing to remind the police to work professionally on the cases she experienced were part of the challenges faced by GBVO victims while seeking justice through the legal process.

On the other hand, it is interesting to pay attention to the results of the decisions in the Kennedy case. Judges through Court Decision Number 281 / Pid.Sus / 2019 / PN JktPst decided the perpetrator was guilty of the charge of distributing content with violations of decency in accordance with Article 27 Paragraph 1 of the ITE Law, and Article 93 of the Population Administration Law regarding falsification of population documents to implementing agencies. As is well-known, Article 27 Paragraph 1 of the ITE Law is an article that ensnares Nuril and E. This confirms the catchall element on the article, especially in the charges on the decency.

SAFEnet regrets that the decision of the Panel of Judges did not take into account the charges based on Article 32 Paragraph 1 of the ITE Law regarding information / electronic documents belonging to people or the public that were changed, added, or reduced. This article was encouraged by LBH Jakarta, as Kennedy's attorney, because the KBGS that Kennedy experienced also occurred because there was an attempt to disseminate Kennedy's cellphone number by changing the information with incorrect information regarding ownership of Kennedy's cellphone number.

Anyone knowingly and without right or

against the law in any way changes, adds, reduces, transmits, destroys, removes, transfers, hides Electronic Information and / or Electronic Documents belonging to other people or public property. - Article 32 Paragraph 1 of the ITE Law.

Another challenge comes from the side of law enforcement officers who do not yet have a perspective to support victims. Instead, law enforcement officials often blame the victims for the GBVO they face. This happened to F¹³, who was accompanied by SAFEnet in the process of reporting to the police regarding KBGS in the form of threats to spread intimate content with the motive of extortion (sextortion). During the process of making the Investigation Report, F found herself being asked about the things that lead to victim blaming, so that the victim was traumatized and felt slumped until she thought of committing suicide.

On the other hand, while providing assistance, SAFEnet also found reasons such as "limited human resources" and "lack of tools" for digital forensics or tracking to the police are often raised when it was pushed for case investigation. The reason that is also a challenge raised by law enforcement officials is that it is difficult for them to get information about the perpetrator if they ask the digital platform, even though the digital platform already has a special policy related to reports by law enforcement officials.

Another case that has received public attention is related to two videos with sexual scenes of more than two people sold by a Twitter account. The video went viral with the hashtag G¹⁴ on Twitter in August 2019. G, who was 19 at the time, was immediately detained by investigators until she became a defendant in a trial at the Garut District Court with the Public Prosecutor filing Article 8 Jo of the Pornography Law. Article 34 Jo. KUHP Article 55 Paragraph 1 to ensnare G.

Every person is prohibited from deliberately or with his/her consent from becoming an object or model that contains pornographic content. - Article 8 of the Pornography Law

Convicted as a perpetrator of a criminal

¹³ Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

¹⁴ Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

act: 1. those who commit, order to do so, and who participate in the act. - KUHP Article 55 Paragraph 1

It is known that in April 2020, G was found guilty¹⁵ of fulfilling the element of “deliberately participating as an object containing pornographic content” in the decision of the Garut District Court Number 289 / Pid.B / 2019 / PN.Grt. However, if you look deeper into this case, G is a victim of sexual exploitation by the perpetrator who is her ex-husband.

G experienced sexual violence, starting from being forced to have sex with a man other than her ex-husband, deliberately being recorded, until the video was sold via the Internet. In the production of video content labeled as pornographic products, G did not give full consent because she was under intimidation from her ex-husband who had deviant sexual behavior. Especially in the process of distributing the video content which is monetized by the actors, it should also be noted that the age difference between the two is 14 years, and the perpetrator has married G since she was 16 years old, so it is clear that in their relationship there is already an imbalance of power relation.

The decision of the Garut District Court shows again the vulnerability of women in being victims of sexual violence coupled with GBVO when dealing with the law, even when there is already Perma No. 3/2017 concerning Guidelines for Adjudicating Cases of Women in Conflict with the Law and recommendations for ending legal bondage to G by Komnas Perempuan.¹⁶

The lengthy legal process also does not address the characteristics of “online” or “digital-facilitated” technology which is fast in the dissemination and multiplication of content. There are stuttering, unresponsive, and unprepared law enforcement officials to resolve GBVO cases, both from the reporting stage to the trial. Time-consuming legal procedures also expose victims to recurrent

violence, with the number of perpetrators likely to increase. In KBGS, in the form of dissemination of intimate content, victims must be prepared to face the big risk that the content can be uploaded repeatedly by the main perpetrator, and by other actors who find the content and use it to further intimidate the victim. This has an impact on the psychological condition of the victim and the victim’s recovery process.

Solutions not yet end in justice

In assisting the KBGS case, SAFEnet also helps the reporting process to the digital platform and faces its own challenges. In some situations, it was found that victims or survivors had minimal understanding of the reporting procedures to the digital platform, so they needed reporting assistance.

Victims, survivors, and SAFEnet as companions also had times when the reports to the digital platform got unsatisfactory results. Oftentimes the reports are rejected because the reporting feature on the digital platform is not responsive to events experienced by the victims, so the reports do not result in deleting the content uploaded by KBGS actors or accounts created by the perpetrators. Instead of being deleted, the reason that is often conveyed is that the digital platform finds no violation from the content to the standard community guidelines or the terms of using digital platforms.

On the other hand, digital platform providers, such as social media giants Facebook, Instagram, Google, Twitter, have systems or features that facilitate perpetrators to easily distribute content or create dozens of new fake accounts, so that when victims wait for the digital platform to respond the reports, they are still vulnerable to be re-attacked with the uploaded content or new accounts created by the perpetrator.

Another feature that contributes to the vulnerability of victims is the ability of it to duplicate content through public API (application programming interface) provided by several digital platforms, such as Instagram and Twitter, so that data uploaded to this digital platform can be duplicated by

¹⁵ The verdict is currently under appeal at the Bandung High Court at the time this report was written.

¹⁶ Iqbal, M. (2019, September 20).. Accessed from Merdeka on 16 Juni 2020 <https://www.merdeka.com/peristiwa/berbekal-surat-komnas-perempuan-pengacara-minta-polisi-hentikan-kasus-vina-garut.html>

third parties automatically.

Related to the use of public APIs that contribute to vulnerability to victims of GBVO, this occurred when SAFEnet accompanied the case of B, in which B's intimate content appeared in Google search engine results in the form of duplicated images from public posts on Instagram and Twitter to the site <http://pictame.biz/>, <http://saveig.org/>, dan <http://terasocial.com/>¹⁷. All three function similarly to the ImglInn example above.

Removing this content is not easy, even after coordinating with the digital platform that publishes the public API, because it is connected to third parties using the API, as well as reporting to Google which brings up the content in its search results.

This handling of digital content reporting is not only tangled in matters like the above, but also in the case facing Kennedy. She only managed to contact one digital platform, namely BeeTalk, because they have offices in Indonesia, while WeChat and Badoo cannot be contacted because they do not have a representative office in Indonesia.

Monetization and Normalization of KBGS in Mass Media!

When talking about KBGS, there is a need to also discuss the role of online mass media. Mass media plays an important role in building social change, educating the public, and also encouraging public policy. Unfortunately, SAFEnet, through observations of 22 posts with the tag #WTFMedia by the @magdaleneid Instagram account¹⁸ during 2019, found that online mass media often objectified women's bodies and perpetuated the normalization of KBGS with sensational stories aimed for click-bait with orientation of monetization. Titles like these often do not represent the perspective or are sensitive to issues or groups that have vulnerabilities related to gender, sexuality, and violence they experience.

On the other hand, sensational and lacking-empathy reporting has the potential to become a new GBVO, such as when it neglects to pay attention to the vulnerability and privacy of victims, for example when revealing personal data such as name and location. For examples, taking the form of deadnaming, or spreading to the public the real name of a transgender person without their consent. The impact can be long, especially given the vulnerability of transgender people in Indonesia as a minority group that are often subjected to discrimination.

Violations of privacy and non-consensual activity regarding a person's personal data, gender and sexuality are at the root of gender-based violence. With the Internet and / or being facilitated by digital technology which has certain characteristics, such as fast spreading, easily duplicated and produced content, and its lasting footprint; gender-based violence has impacts that were unthinkable before. The online mass media should not be the party or actor that contributes to adding to the vulnerability and risk of the occurrence of KBGS.

Women and Digital Body that Must Compromise

Talking about gender and sexuality, Indonesia still adheres to a strong patriarchal culture and perspective, so that oftentimes the bodies of women or non-binaries that are practiced become targets that are regulated by adherents of this culture. Thus, when this culture and perspective is carried over into behavior in the digital world, other bodies in this digital world are also regulated for the same reason. Seeing this, it is not surprising that the majority of GBVO victims are women and bodies that identify with other identities, such as non-binaries.

It is also not surprising to hear when a statement from the Ministry of Communication and Information (Kominfo) emerged in July 2019 which said that they asked Google's digital platform (Alphabet), where YouTube is under its umbrella, to block three contents belonging to Youtuber and

¹⁷ These three websites are no longer accessible at the time of writing of this report.

¹⁸ This account is managed by Magdalene, an online mass media with the claim of "Indonesian Feminist Webmagazine"

Gamer H¹⁹ on the grounds that H's YouTube content was suspected to violate the elements of decency contained in the ITE Law Article 27 Paragraph 1.

In the beginning, there were reports of complaints from the public regarding content produced by H that are uploaded to her YouTube channel. It is also known that H's content was also reported through an official request from the Chairman of Commission I of the Indonesian Parliament Abdul Kharis Almasryhari at the Hearing Meeting which took place on 18 July 2019. Through an independent investigation by the AIS Kominfo Team, 9 contents allegedly violated decency were found. YouTube was asked to block 3 content and activate the restriction feature for viewers aged 18 and under for 6 other videos, which was then carried out by the digital platform.²⁰

Indonesia
Request
We received a request from the Ministry of Communication and Information Technology to remove 9 YouTube videos from a popular Indonesian YouTube creator for containing allegedly sexually provocative gaming content.
Outcome
We restricted access to 3 of the videos from YouTube in Indonesia and age-restricted the remaining 6 videos from view by users under the age of 18.

Picture 1 Google Transparency Report for the period July 2019 - December 2019

The incidents including GBVO show again the catchall element at the ITE Law Article 27 Paragraph 1, which this time is used to repress women's expression and sexuality in the digital world. SAFEnet sees patriarchal culture and perspective accompanied by "male gaze" in interpreting this element of decency will continually narrow the space for women's expression and make their digital bodies to continue to compromise, if they still want to use digital spaces, which are actually no longer safe for them. The impact is not only on women's voices or expression spaces, but can affect women's economic

factors, in this case H as a content creator.

Homework for collaborating in Handling KBGS

Reflecting on the complaint of the KBGS case, it is important for various stakeholders to sit down together and collaborate in handling the GBVO case. Digital technology or the Internet are not the only factors that contribute to KBGS. There are many contexts from various perspectives that make this violence occur, and especially gender-based violence is the context of deep-rooted patriarchal and power relations structures that contribute greatly to the cause.

Therefore, handling GBVO in Indonesia is the homework of all stakeholders involved in the scope of digital and online technology itself, from users, digital platform providers, law enforcement officials, to policy makers.

In 2019, SAFEnet initiated and was involved in several cross-sector and multi-stakeholder focus group discussions (FGD) with victims, NGOs including LBH and counseling agencies, government institutions (related ministries such as Komnas Perempuan, Kominfo, KPPPA, CCIC Polri), digital platforms (social media such as Google, Facebook and Twitter; transportation applications such as Grab and Go-Jek) related to the handling of GBVO in Indonesia.

The process and law enforcement are the main keys that must be reformed in the handling of GBVO. It must be developed so that it can answer the various challenges faced by victims of GBVO, as has been raised in this report. The attitude of law enforcement officers who do not have a victim perspective and have a tendency to blame the victim (victim blaming), also sometimes stutter with digital technology and cyber violence modes, the legal process is long and does not answer the characteristics of online violence or that is facilitated by digital technology, safeguarding evidence, until the evaluation of catchall articles that have the potential to criminalize victims instead of protecting them in the realm of law, such as the ITE Law Article 27 Paragraph 1. A law that has a good victim perspective is needed and must be

¹⁹ Identity disguised. The case is described as a form of education on the variety of KBGS experiences experienced by victims.

²⁰ This report can be accessed at https://transparencyreport.google.com/government-removals/by-country/ID?country_request_amount=group_by:requestors;period:Y2019H1;authority:ID&lu=country_request_explore&country_item_amount=group_by:totals;period::authority:ID&country_request_explore=period:Y2019H2;authority:ID

strictly implemented so that it can advocate for victims who experience GBVO.

Digital platforms must also increase their responsibilities in the form of policies, reporting features and responses, as well as digital technology innovations that anticipate various forms of GBVO. Many digital platforms are increasingly integrated with each other, connectivity between mobile applications is getting higher, cross-platform and multi-platform content sharing features are becoming easier and smoother to do, but the content reporting features fronted by each digital platform still experience stuttering and have an impact on digital traces that haunt the victims of the GBVO. A digital platform with an orientation that makes it easier to share content and data, must also create a friendly and accessible space for users in terms of security and privacy settings, as well as reporting features that are more responsive to the needs of victims.

SAFE-net also recommends capacity building and insights related to digital security for victim assistants, for example through training in the form of workshops or digital security training. In addition, there needs to be education for citizens, for example by increasing news coverage in the mass media with a gender and sexuality perspective and supporting reporting practices that promote the privacy of the subject being reported, or by adding a curriculum related to GBVO for various school levels, from elementary school to College. This will also help to equalize access to information on assistance for victims of GBVO.

Note:

SAFE-net has obtained approval to describe the KBGS experienced by victims and survivors whose identities are disguised as A, B, C, D, E, and F as a form of education to the public. SAFE-net has also obtained the approval of Baiq Nuril Maknun and Kennedy Jennifer Dhillon to write their names in this report. They are part of the victims and survivors who were

and are still assisted by SAFEnet in their case advocacy. The description of cases G and H is based on observations from news and various other sources.

Digital Attacks Target Groups at Risk

Digital attacks are starting to become a serious problem that activists, journalists, women and groups at risk in Indonesia must face. There have been various forms of digital attacks, ranging from impersonator accounts, doxing, persecution, using hoaxes as weapons (weaponization of social media), hacking, to illegal tapping (unlawful breach and illegal surveillance). Digital attackers can come from state hackers, dangerous groups, to individuals as terrorists. Usually digital attacks are directed at activists, journalists, women and vulnerable groups occur at the momentum of social and political events taking place in Indonesia.

During 2019, SAFEnet received a number of reports of digital attacks experienced by academics, anti-corruption activists, and student activists involved in the issue of the KPK Law Revision and #ReformasiDikorupsi.

One of them happened in Yogyakarta. Around the first week of September 2019, UGM lecturer Professor Rimawan Pradiptyo made a consolidation movement and coordination through the UGM Integrity Whatsapp group to gather around 2,000 lecturers from 34 universities. About 4-7 days later, professor Rimawan received an SMS from Pizza Hut Delivery sending the booking code XXX. Two minutes later a similar SMS was sent with an activation code. Later, a SMS notification from Whatsapp came in notifying that his cellphone is no longer connected to Whatsapp. Then a notification appeared that another number 087XXX had controlled the Whatsapp account.

About an hour later, professor Rimawan received news that his Whatsapp account was sending messages to the entire Whatsapp Group with a clickable link that would lead to a site that supports the revision of the KPK Law. Due to the disturbance, he asked the Whatsapp group to be disbanded and form a new Whatsapp group by inviting

old members. However, at the same time a WA Group appeared with more or less the same name and invited other members so that finally all members left the group.

In addition, the next day around 02.30 WIB, Professor Rimawan continuously received spam/robo calls from country code +1 (United States). UGM lecturer and anti-corruption activist Oce Madril also experienced a similar incident. Oce received a kind of notification via SMS (can't remember the exact content of the notification) from Whatsapp even though he never made a request. Then Oce also received intensive calls, mostly with the country code +1 (United States), +61 (Australia), and numbers from African countries.

The spam / robo call occurred when Oce was conducting a press conference or other schedule related to organizing activities. This spam / robo call occurred from morning to evening and did not stop. Often times spam / robo calls occur at important moments, be it a press conference or demonstration. As Oce recalls, this incident occurred intensively for one week. Apart from Whatsapp, at the end of September 2019 there was also an attempt to take over the Telegram account, but because there was a notification from Telegram about attempts to log in from an unknown device, finally this could be mitigated. Professor Rimawan said that the digital attacks he experienced had an effect on the consolidation of the anti-corruption movement from academia.

Reports of digital attacks also occurred in Bandung. Bigwantsa Nuary and Luthfi Indrawan, Unpad students majoring in Public Administration are both active in the Unpad Student Consolidation (KMU). Accompanied by one of the Unpad graduates, they actively voiced a motion of no confidence in relation to the rejection of the KPK Law Revision and the #ReformasiDikorupsi movement.

According to Lutfi, the digital attack started with the occurrences of a number of One-Time Password (OTP) requests that he never asked himself to Whatsapp. It was recorded that OTP requests entered the SMS inbox on September 15 at 11.20 PM (23.20 WIB), then second OTP request was sent on September 16, 2019 at 12.00 PM (00.00 WIB), and one OTP

sent on the same day at 10.55 AM (10.55 WIB). In addition, Lutfi also received a request to enter the 2VA code at 02.50 WIB which he never remembered to activate.

It turns out that his Whatsapp account sent messages that were spread to a number of campus Whatsapp groups and their families around 02.08 WIB with provocative sounds. In addition, one of the graduates who was actively helping the two of them also confirmed that his Whatsapp account had spread messages similar to what happened to Bigswansta.

Based on reports that have been submitted during that period, SAFEnet found similar patterns experienced by academics, anti-corruption activists, and student activists involved in the issue of the KPK Law Revision and #ReformasiDikorupsi. First, the digital attack took place around September - October 2019. Second, the digital attack was closely related to the involvement of the reporters in the protest against the KPK Law Revision. Third, digital attacks are directed because of their crucial position in the movement to reject the KPK Law Revision. Fourth, digital attacks are used to weaken the consolidation and movement they are carrying out.

Technology Oppression in Handling Papua Issues

In 2019, Facebook issued a finding on the practice of Coordinated Inauthentic Behavior (Unauthentic Behavior Coordination) in Indonesia. Facebook's Head of Cybersecurity Policy, Nathaniel Gleicher, explained that CIB is a behavior that is categorized as abuse. CIB is a coordinated action of a number of FB Pages / accounts that work together to trick others about who they are and what they do. CIB actions can be carried out for ideological purposes or because of economic motives. He added that Facebook deleted these accounts not because of their content, but because of their behavior that deceived others. Its content may not violate the terms of the Facebook Community Guidelines.

The two CIB findings occurred on 31 January 2019 and 3 October 2019. In the second

discovery, Facebook deleted 69 Facebook accounts, 42 Facebook Pages, and 34 Instagram accounts that were involved in coordinated inauthentic behavior in Indonesia. The people behind this network use fake accounts to manage Facebook Pages, spread their content and redirect people to websites off the platform. They mainly posted in English and Indonesian about West Papua with some Facebook Pages sharing content in support of the independence movement, while others posted criticism of it.

Although the people behind these activities tried to hide their identities, a Facebook investigation found a link to a company in Indonesia called InsightID. A Facebook report says InsightID manages 69 Facebook accounts, 42 Pages and 34 Instagram accounts. There are around 410,000 accounts following one or more of these FB Pages and around 120,000 accounts following at least one of these Instagram accounts.

InsightID also spent about \$ 300,000 (equivalent to Rp 4.2 billion) spent on paid Facebook ads.

Investigations in the digital realm of InsightID have been carried out since the report was made to this day and so far, profiling can be gathered - despite the tremendous effort to erase all of InsightID's digital track record and the people who work behind it. InsightID is a startup company in the form of an individual consulting services agency that was formed in February 2018.

Just as corporate websites are removed and disguised, digital traces to InsightID-managed websites are also deleted.

Platform manipulation has also been found in the form of deploying trolls and bot accounts to attack residents who comment on events in Papua. These bot and troll accounts act mechanically and spread the same message over and over.

On 22 November 2019, SAFEnet also received a complaint about the DDoS attack on the collective work of a number of Papuan human rights workers in Jakarta, Papua and abroad who collected data on Papuans imprisoned on the Papuans Behind Bars website with

URL <https://www.papuansbehindbars.org/>

When we checked the server, it was found that the target of this massive DDoS attack was the Papuan Behind Bars website. This DDoS attack was accompanied by attempts to hack Telegram, Whatsapp accounts and takeover Gmail accounts from one of the human rights defenders involved in the website.

In the technological oppression carried out against activists, human rights defenders and journalists working on the issue of Papua, SAFEnet highlighted the re-occurrence of doxing practices that had been rampant in 2017 in the Ahok Effect incident. Doxing is the process of gathering identifiable information about a person or group of people, with the aim of humiliating, frightening, blackmailing, slandering, bullying or harming a target.

Publicly posting someone's personal details is often done with the intent of harming the targeted individual, especially if the person is a law enforcement officer, an undercover agent or a well-known individual. Furthermore, a doxing is likely to drag family and sometimes friends of the target, sometimes including children.

It is illegal to post personal information publicly with the intention of embarrassing, defaming, harassing or harming. This puts doxing individuals in a potentially dangerous situation.

During 2019, doxing happened to human rights defenders and journalists related to sensitive issues in Papua. In October 2019 at 04.35 WIB, the Twitter account @digeembok carried out doxing against Papuan human rights defender Veronica Koman by notifying the location where Veronica Koman's parents lived. This doxing attempt was accompanied by intimidation that Veronica Koman had been monitored by the account.

In addition, three journalists covering the Papua issue experienced doxing. In August 2019, the Twitter account @antilalat doxed 3 journalists through their posts.

Then in September 2019, Febriana Firdaus, Aljazeera journalist, also experienced doxing

because of his reporting regarding the number of victims who died in the riots in Papua.





Epilogue: Fight Back Digital Authoritarianism

Even though Indonesia is no longer led by an iron-fisted figure like the New Order regime under Soeharto, the shadow of this authoritarian power still grips the heads of many people. Imagining the return of military dual function, tight information control, uniformity in many dimensions in order to perpetuate corrupt, collusive and nepotic power, is a scourge that can also be felt today, even though Suharto was overthrown more than 20 years ago in 1998.

During the 2019 presidential election, the anti-New Order narrative was present considering the presence of Prabowo, one of the presidential candidates who was close to the Suharto family circle. Meanwhile, another presidential candidate who is currently elected for the second time, Joko Widodo, said that he had no burden. However, activists criticize that whoever wins the general election, it is almost certain that they are supported by the power of the oligarchy which is still closely related to the New Order. This is what is behind the #SayaGolput movement ahead of the 2019 general elections in Indonesia.

Joko Widodo won the 2019 general election again by a narrow margin. The public, which had been split due to the polarization of support, had thickened negative sentiment, by taking a move to reject the election results in the form of demonstrations in front of the Election Supervisory Board (Bawaslu) in Jakarta. The demonstration then became uncontrollable and culminated in heavy restraint from the security apparatus. The heated atmosphere, which started with the rejection of the election results, became violent eruptions between Prabowo supporters and the police.

Then, for the first time in Indonesia, there was a slowdown in the Internet (bandwidth throttling) on 23-25 May 2019. The government's reason at that time, as stated in a press release by the Ministry of Communication and Information, was to prevent hoaxes related to riots from circulating. Of course, this incident is surprising, considering that bandwidth throttling is a form of technological oppression that has been criticized by many parties, including the United Nations, for

violating international law regarding the right to access information.

Criticism from civil society organizations, including by SAFEnet, has gone unnoticed by the government regarding the lack of due process of law and transparency of action. In fact, this Internet slowdown was carried out again in August, and was followed by an Internet shutdown until September 2019 in Papua and West Papua. On many occasions, the Indonesian government has boasted that what they have done has been praised by many countries for being able to balance freedom of expression and national security.

After the 2019 general election, the Joko Widodo administration, supported by the oligarchy, consolidated with its political opponents by giving ministerial and other strategic positions. The Indonesian government focuses on investing and improving human resources (HR), as stated in the presidential speech, and has made no mention of protecting human rights (HAM). To support investment needs, the president has made every effort, including security forces and intelligence, to pave the way, especially to launch his efforts to pass the Omnibus Law. In addition, the government has also proposed a revision of the Corruption Eradication Commission Law (KPK Law), which one of the points asks for a KPK Supervisory Board to oversee the performance of this anti-corruption agency. These two policies were considered critical by civil society organizations and academics as an effort to weaken the power in fighting corruption and oligarchy. Therefore, there were massive demonstrations related to rejection of the revision of the KPK Law and also the Omnibus Law in many cities.

The demonstration, which was mostly carried out by students, academics, and activists, met with violence in a number of cities. Hundreds of victims were reportedly injured as a result of clashes with the authorities, and there were even victims who died. Physical violence was exacerbated by reports of digital violence experienced by students, academics and activists. In addition, with the escalation of the conflict in Papua due to racial actions against Papuan students in Malang and Surabaya, physical and digital

violence has also occurred against those who advocate the issue of Papua, followed by Internet slowdown and Internet blackout.

Hacking incidents of activists and academics, intimidation in the form of doxing to activists and journalists, deploying a cyber army led by key opinion leaders to attack opponents of government policies, as well as critical media, are signs of how technology is used to repress freedom of expression and independence to gather in Indonesia.

Complete records of all these incidents have been monitored and included in this year's report on the condition of digital rights in Indonesia to be read. As an organization that fights for digital rights in the Southeast Asia region, including Indonesia, SAFEnet is truly worried that Indonesia will soon catch up with many countries in the region that are now practicing Digital Authoritarianism.

Since Edward Snowden disclosed the mass surveillance programs run by intelligence agencies in Western democracies in 2013, the facts show that digital authoritarianism practices do not solely occur in authoritarian regimes. This kind of thing can happen even in democratic countries. Manipulation of digital technology as well as misuse of social media and algorithmically curated news feeds can be used to undermine a country's democratic values.

What will happen, as can be seen in authoritarian regimes, is how digital communication technology is used to filter and censor to control the flow of information in and out of the country. State-sponsored actors use wiretapping, cyberattacks and disinformation to consolidate power. In addition, among their fellow authoritarian regimes they exchange tools and expertise in controlling the Internet and promote ideas on how to regulate digital technology at the international level, as Professor Diebert calls Network Authoritarianism as has happened in China so far.

Adopting the disaster system that has been used so far in preparing reports on the condition of digital rights, SAFEnet has determined that Indonesia is now in a state of alert to face Digital Authoritarianism.

Realizing the situation of the rise of Digital Authoritarianism, there is no other way that we can recommend, apart from fighting back to beat back the emergence of digital authoritarianism in Indonesia, through legal channels, criticizing openly, consolidating civil society at the national level, while also building support from the region and international to prevent the worst in the future.



SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

2020