

Indonesia Digital Rights Situation Report 2020

# DIGITAL REPRESSION AMID THE PANDEMIC



Indonesia Digital Rights Situation Report 2020  
**Digital Repression amid the Pandemic**

**Team**

Patron: Damar Juniarto

Coordinator & Editor: Anton Muhajir

Writers:

A. Ryan Sanjaya

Abul Hasan Banimal

Bimo Fundrika

Ika Ningtyas

Nabilla Saputri

Nike F. Andaru

Nenden Sekar Arum

Supriyono

Unggul Sagena

Cover Illustration: Abul Hasan Banimal

Design & Layout: Syamsul Arifin

English Translators:

Supriyono


Bani Nawalapatra

English Editor & Proofreader: Ravio Patra



Southeast Asia Freedom of Expression Network (SAFEnet)

Jalan Gita Sura III Nomor 55 Peguyangan Kaja

Denpasar, Bali 80115

 +628119223375

 [info@safenet.or.id](mailto:info@safenet.or.id)

  @safenetvoice

 [safenet.or.id](http://safenet.or.id)

# CONTENTS

<b>4</b>	Foreword
<b>6</b>	Profile
<b>10</b>	Executive Summary
<b>16</b>	Data and Analysis
<b>16</b>	Internet Access
<b>32</b>	Freedom of Expression
<b>46</b>	Digital Security
<b>64</b>	Epilogue

# FOREWORD

A year has passed since the COVID-19 pandemic hit. As of March 2021, the disease has killed more than 2.69 million people worldwide, including in Indonesia, and continues to spread fear. While vaccines to curb the spread of the disease has been discovered and are being rolled out, there are still no signs that the pandemic will soon end. Same goes to the pandemic impact on digital rights.

Over the course of the past year, the COVID-19 pandemic has had a significant impact on digital rights in terms of internet access, freedom of expression, and digital security. Our year-long monitoring shows that the COVID-19 pandemic has led to an increase in repression through, or on, digital media platforms.

The steep rise of digital rights violations amid the COVID-19 pandemic makes the publication of this Indonesia Digital Rights Situation Report exceptionally relevant. Since 2018, the publication of this report annually has become a crucial part of our works in advocating for digital rights in Indonesia beyond the documentation of data and facts.

This report specifically focuses on how the COVID-19 pandemic has impacted digital rights as well as on the overall digital rights situation throughout 2020.

In developing this report, we collected and analyzed a set of primary and secondary data. Primary data are collected through our monitoring activities throughout the year with information coming directly to our hotline and reporting center as well as observation of the mainstream media and social

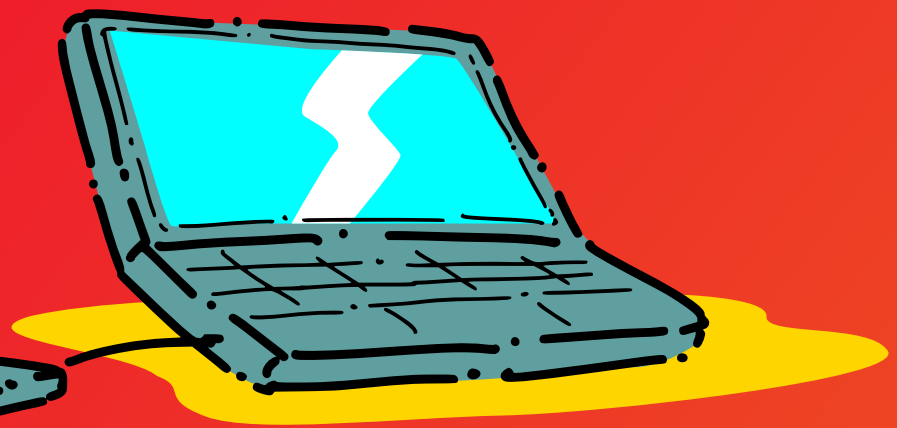
media platforms, whereas secondary data are collected from information published by both government and civil society stakeholders who also conduct digital rights monitoring. We also conducted interviews with victims of incidents related to freedom of expression and digital security.

This report is presented in three main sections: the right to internet access, the right to freedom of expression, and the right digital security. This reflects the same three major thematic areas that have guided our works at SAFEnet for the past three years. To conclude the report, we wrote an epilogue to reflect on and recommend a way forward in response to the findings of this report.

We hope that this report could serve as an ammunition to further campaigns for digital rights, as increasing reliance on digital media should be followed by the fulfillment of digital rights as a human right.

It is also our hope for this report to be used as a reference and an advocacy tool by all digital rights stakeholders in Indonesia and globally. This includes proponents of other individual rights such as the right to privacy and the right to freedom of expression as well as human rights and democratic freedom. Enjoy the read.

Denpasar, April 2021.



## PROFILE

The Southeast Asia Freedom of Expression Network (SAFEnet) was established on 27 June 2013 in response to rampant criminalization against internet users in Indonesia following the implementation of Law No. 11 of 2008 on Electronic Transactions and Information (ITE Law). To date, SAFEnet has continued to advocate for victims of the ITE Law, particularly in defense of the critical voices who use the internet as a tool to express and make opinions. During its first five years, SAFEnet had focused on the issue of freedom of expression in the digital space.

Since 2018, SAFEnet began to expand its advocacy goal to cover the broader theme of digital rights, which include the right to internet access, the right to freedom of expression, and the right to digital security. In January 2019, SAFEnet was registered legally as the Association of Southeast Asia Freedom of Expression Defenders and is based in Denpasar, Bali.





*SAFEnet actively supports victims of the ITE Law criminalization, such as in the trial of Saiful Mahdi, a lecturer at Universitas Syiah Kuala, Banda Aceh, sued for defamation over a chat group message.*

### **Vision**

To create an inclusive and safe digital space for everyone regardless of their political identity, ethnicity, religion, gender, sexual orientation, and physical abilities.

### **Mission**

- To fight for digital rights, encompassing the right to internet access, the right to freedom of expression, and the right to digital security,
- To advocate for policies and support victims of criminalization and digital attacks enabled by information technology, and
- To stand in solidarity with civil society fighting for human rights in the digital space.

### **Strategy**

To realize its vision and mission, SAFEnet combines three main approaches: monitoring, advocacy, and solidarity with civil society in support of members of the general public and specifically those classified as human rights defenders actively using digital media platforms as an advocacy tool.

## **Institutional Structure**

Formally, SAFEnet is comprised of three components: supervisors, executives, and volunteers.

SAFEnet supervisors are civil society members with extensive experience in the areas of internet governance, digital literacy, and digital security.

SAFEnet executives and volunteers work separately in various cities in Indonesia, including Pekanbaru, Palembang, Jakarta, Bogor, Yogyakarta, Semarang, Surabaya, Banyuwangi, Pontianak, Samarinda, Denpasar, Makassar, Ambon, and the Papua region. As of March 2021, SAFEnet is supported by over 40 volunteers across 23 cities. They come from diverse backgrounds, such as journalists, bloggers, housewives, LGBTQ groups, private workers, digital security practitioners, and so on.

## **Programs & Activities**

Since 2013, SAFEnet began monitoring digital rights violations, providing assistance for victims of digital rights violations, and facilitating capacity building initiatives for members of civil society in digital rights.

Some of these activities have included digital rights training for SAFEnet volunteers, monitoring and assistance for victims of the ITE Law criminalization, monitoring and assistance for victims of digital attacks especially high risk groups, capacity building initiatives for members of civil society in digital security, monitoring and assistance for victims of online gender-based violence, advocating for cyber policies, conducting research on hate speech in the digital space, networking with civil society at the national, regional, and international levels, as well as publishing periodic reports on digital rights situation.

## **Achievements**

In the eight years since its inception, SAFEnet has recorded many success stories in defending digital rights alongside partners and allies. This includes securing a Presidential amnesty for Baiq Nuril, a victim of the ITE Law, winning a lawsuit against the President and the Minister of Communication and Informatics regarding the 2019 internet shutdown in



Papua, facilitating the formation of the Association of Victims of the ITE Law (Paku ITE), initiating the formation of the Quick Reaction Team (Trace) as a collective to deal with digital attacks on civil society, and maintaining an active presence at the national, regional, and international stages speaking on digital rights issues.

SAFEnet is also a trusted partner to several digital platforms, such as Google, Facebook, and Twitter, in the mission to create a friendlier and more inclusive internet for all.

### **Supporters & Networks**

In implementing its programs and activities, SAFEnet has received support from many donors, international organizations, and partners. This includes AccessNow, the Association for Progressive Communication (APC), the Digital Defenders Partnership (DDP), Facebook, Ford Foundation, Goethe Institute, Google, ICT Watch, Internews, the International Foundation for Electoral Systems (IFES), and the British Embassy in Indonesia.

At the regional and international levels, SAFEnet is actively involved in the wider movements for digital rights, such as the Keep It On Coalition, the Digital Rights Litigation Network, and the ASEAN Regional Coalition to Stop Digital Dictatorship.





## EXECUTIVE SUMMARY

The COVID-19 pandemic has not only affected our health, but also changed how we go about our days. We have had to adopt new behaviors both in terms of maintaining personal health and hygiene as well as in terms of interacting with the people around us. The normalcy of socializing, gathering in crowds, are being replaced by distancing measures in isolation.

A year since the pandemic turned the world upside down following the first reported case of COVID-19 in Wuhan, China, isolation has now become the new normal. Even when we gather in groups in the same room, we need to keep our distance and cover our faces so as not to further spread the virus.

Fortunately, information technology is here to make it easier. Online digital spaces are growing fast to substitute physical encounters. Physical distance disappears with internet connection. School, work, and even religious worships have now moved to our very own personal spaces. The internet makes it all possible.

However, not everyone can access the opportunity. The privilege of studying, working, attending worships, and going on with our daily activities online can only be enjoyed if one has access to resources both in terms of equipment and capacity. The *Indonesia Digital Rights Situation Report 2020* breaks down the importance of fulfilling digital rights amid the pandemic as well as presents evidence on how inequality persists and renders citizens more vulnerable, especially the critical voices.

The COVID-19 pandemic has exposed the inability of the Indonesian government to fulfill the digital rights of its citizens.

### **Right to internet access**

To prevent the spread of COVID-19, many countries have imposed lockdowns or restrictions so that people must carry out their activities from home, including work, study, and religious worship. However, reliable and speedy internet access is not available to all. Many residents, especially those of lower economic class and those li-

ving in remote areas, are still struggling to get proper internet access despite the steady increase in internet penetration rate.

In the second quarter of 2020, the number of Indonesian Internet users reached 196.7 million people or 73.7% of the population, up from the 64.8% recorded in 2018–2019 according to the Indonesian Internet Service Providers Association. Another source recorded a slightly different number of users at 202.6 million people albeit at a similar rate of 73.7%. Meanwhile, access from mobile devices reached 345.3 million (125.6%), indicating that each person in Indonesia owns 1–2 mobile devices.

Social media penetration also continues to rise with 170 million users as of early 2021, an increase of 6.3% from the previous year. YouTube is the most popular platform in the 16–64 age category with a 93.8% market share, followed by WhatsApp (87.7%), Instagram (86.6%), Facebook (85.5%), and Twitter (63.6%).

However, the increase in penetration does not go hand in hand with equal distribution of internet access. Some residents remain unable to conduct their activities from home due to inadequate infrastructure, economic limitations, and low capacity.

The Ministry of Education and Culture issued Circular No. 15 of 2020 to guide the implementation of online and of-

online distance learning program during the pandemic. However, the policy fails to address the unequal distribution of internet access and infrastructure. Among others, it is estimated that about 12,000 schools do not have access to electricity and about 42,000 are not connected to the internet. Meanwhile, among the ones that do have internet access, about 48,000 are of poor quality.

On the other hand, many students do not own smartphones or other devices to access the internet. And when they do have one, some cannot afford the internet data package or are unable to operate the software used in distance learning.

In addition to problems in the education sector, limited internet access amid the pandemic has also worsened the fulfillment of economic rights for some citizens. While the government encourages businesses to digitize, those categorized as micro, small, and medium enterprises face further obstacles relying on relatively expensive, unstable, and unfairly distributed internet access.

As relief for affected residents, the government introduced the Pre-Employment Card Program and distributed social assistance. And yet again, limited internet access continues to be a barrier as registration for the Pre-Employment Card Program is conducted online.

Furthermore, our findings highlight how limited and unfairly distributed access to the internet cause an even more severe negative impact on the digital rights of minority groups, particularly Papuans and international refugees.

### **Right to freedom of expression**

Criminalization against internet users using the ITE Law has intensified as well during the COVID-19 pandemic. The government justifies this as a response to curb the spread of hoaxes and hate speech. Particularly problematic is how the government tends to label any information that is not in line with its messaging on COVID-19 response as hoax, leading to an increase in legal charges against many citizens.

Throughout 2020, SAFEnet recorded at least 84 criminal cases against netizens, almost four times higher than the 24 cases recorded in the year prior.

The ITE Law remains a looming threat against the freedom of expression of netizens, with 64 of the 84 cases citing problematic articles of the Law, particularly Article 28 (2) on hate speech in 27 cases, Article 27 (3) on defamation in 22 cases, and Article 28 (1) on consumer loss due to false information in 12 cases.

In addition to the ITE Law, several other regulations are noticeably being used as well to limit expression in the digital space. Articles 14–15 of Law No.

1 of 1946 on riots are cited in at least 21 cases along with Articles 207 and 310 of the Criminal Code on insult and defamation.

The victims in these cases are dominated by regular citizens (50) and activists (15), followed by labors (4), university students (4), private employees (3), grade school students (2), and journalist (1). This marks a significant increase from 2019 which recorded criminalization against journalists in 8 cases, activists in 5 cases, and regular citizens in 4 cases.

The steep rise of criminalization against freedom of expression throughout 2020 cannot be separated from two major issues: the government's handling of the COVID-19 pandemic and the controversial passing of the Jobs Creation Omnibus Law.

Also in 2020, the National Police Chief issued official telegrams ST/1100/IV/HUK.7.1.2020 dated April 4 and STR/645/X/PAM.3.2./2020 dated October 2. In the first one, the Chief instructs officers to carry out cyber patrol in order to monitor the circulation of opinion news, targeting the spread of hoaxes regarding COVID-19, the government's pandemic response, and insults against the president and government officials. The second telegram outlined the National Police response toward public rejection of the Jobs Creation Omnibus Law.

**The steep rise of criminalization against freedom of expression throughout 2020 cannot be separated from two major issues: the government's handling of the COVID-19 pandemic and the controversial passing of the Jobs Creation Omnibus Law.**

On November 16, the government also issued the Communications and Informatics Ministerial Regulation No. 5 of 2020 on Private Electronic System Operators. This regulation makes Indonesia one of only a few governments to force social media platforms, online applications, and other online service providers to be liable to local jurisdiction over their content and user data policies and practices. If not properly anticipated, this could potentially exacerbate government repression on freedom of expression.

### **Right to digital security**

In terms of digital security, 2020 also saw a rise in online gender-based violence and digital attacks. Online gender-based violence cases were found to be increasing particularly in families due to increased pressure amid the pandemic. Similarly, digital attacks were on the rise due to massive criticisms toward the government's handling of the COVID-19 pandemic as well as the passing of the Jobs Creation Omnibus Law in October.

Digital attacks can be classified into two categories: a hard attack and a soft attack. A hard attack involves specific skills and equipment to attack a target or even take over their asset. This includes cracking and hacking, tapping, and DDoS (distributed denial-of-service) attacks. Not everyone can carry out hard attacks as it requires specific skills and technology.

A soft attack, on the other hand, is employed to intimidate a target psycho-

logically or publicly damage their credibility. As such, this type of attack must be carried out openly using social media, sometimes anonymously. Examples of soft attacks include doxing, impersonation, and trolling by online mobs. A soft attack is usually coordinated and employs bots and anonymous accounts.

Throughout 2020, SAFEnet recorded at least 147 digital attacks—an average of 12 incidents a month. October saw the highest number of incidents occurring with 41 while only three occurred in March.

Overall, the digital attacks observed targeted mostly government institutions with 38 incidents (25.85%) and regular citizens with 30 incidents (20.41%), followed by journalists with 26 incidents (17.01%), activists with 25 incidents (17.01%), university students with 19 incidents (12.93%), and civil society organizations with 15 incidents (10.20%). The data indicate that critical voices—journalists, activists and university students, as well as civil society organizations—remain the most vulnerable to digital attacks with a combined total of 66 incidents (44.90%).

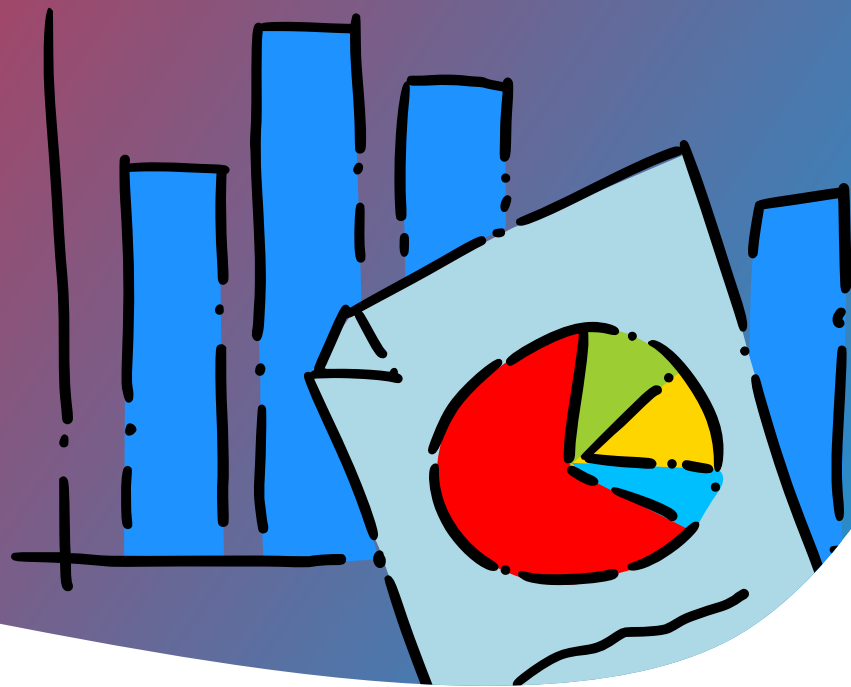
Such finding is reinforced by the fact that digital attacks tend to rise when there is a national political issue dominating public attention. The number of incidents peaking in October could be explained by the massive public protest following the passing of the Jobs Creation Omnibus Law. Likewise,



higher number of incidents in June was very likely connected to the emergence of a movement against racial discrimination toward Papuans and in August 2020 due to intense criticisms over the government's COVID-19 pandemic response.

Our monitoring throughout 2020 reaffirms our previous findings that the digital world remains pivotal for civil society to drive change. Alas, it has also become a means of repression against civil society, including through digital attacks.

**The data indicate that critical voices — journalists, activists and university students, as well as civil society organizations— remain the most vulnerable to digital attacks with a combined total of 66 incidents (44.90%).**



# DATA AND ANALYSIS

## Internet Access

As people move their activities home during the COVID-19 pandemic, the demand for internet connection increased rapidly. However, inadequate infrastructure and economic resources leave some citizens deprived of their digital rights to access the internet.

Low internet access can lead to inequality and have negative impact on economic, social, and cultural rights, such as the right to education and the right to a decent living, especially during a pandemic. Without adequate internet access, students cannot attend their online classes from home. Whereas those who had lost their jobs cannot access information of government's relief programs such as the Pre-Employment Card.

The COVID-19 pandemic shows that internet access continues to become more important for in our daily lives as it is extremely essential for us to be able to access other basic rights, such as education and work. Regardless, internet access has remained scarce for some due to inadequate infrastructure and equipment as well as low capacity.

### Recurring Gaps

The Indonesian Internet Service Providers Association (APJII) noted that internet penetration in Indonesia has continued to increase. Up to the second quarter of 2020, the number of internet users reached 196.7 million people or 73.7% of the population, up from the 64.8% rate recorded in 2018–2019.<sup>1</sup>

Similarly, a January 2021 data reported that the number of internet users had reached 202.6 million people, albeit also representing 73.7% of the population.<sup>2</sup> The same source specified that internet access on mobile devices reached 345.3 million or 125.6% of the population count, indicating that each person in Indonesia operates 1–2 mobile devices.

Social media users also continue to

grow from year to year. As of early 2021, there were 170 million users, an increase of 6.3% compared to the previous year. In the 16–64 age category, YouTube is the most popular platform with more than 170 million users (93.8%), followed by WhatsApp (87.7%), Instagram (86.6%), Facebook (85.5%), and Twitter (63.6%).

Despite these progresses, SAFEnet noted two issues. Firstly, increase in accessibility is still unsatisfactory. Compared to the 10.12% or 27.9 million people growth recorded in internet users between 2018 and 2019, the growth in 2020 could be considered as a regress instead. This is mostly due to the government's asymmetrical approach that prioritizes infrastructure over information access, overlooking factors such as geographic, demographic, and gender conditions.

Secondly, the gap in internet access remains wide. Similar to data recorded in recent years, West Java is still home to the highest number of active internet users with more than 35 million people, while North Kalimantan holds the last rank given its small population of only 600 thousand people.

1 <https://republika.co.id/berita/qjj67h414/survei-apjii-73%-masyarakat-terhubung-Internet>

2 <https://www.slideshare.net/DataReportal/digital-2021-indonesia-january-2021-v01>

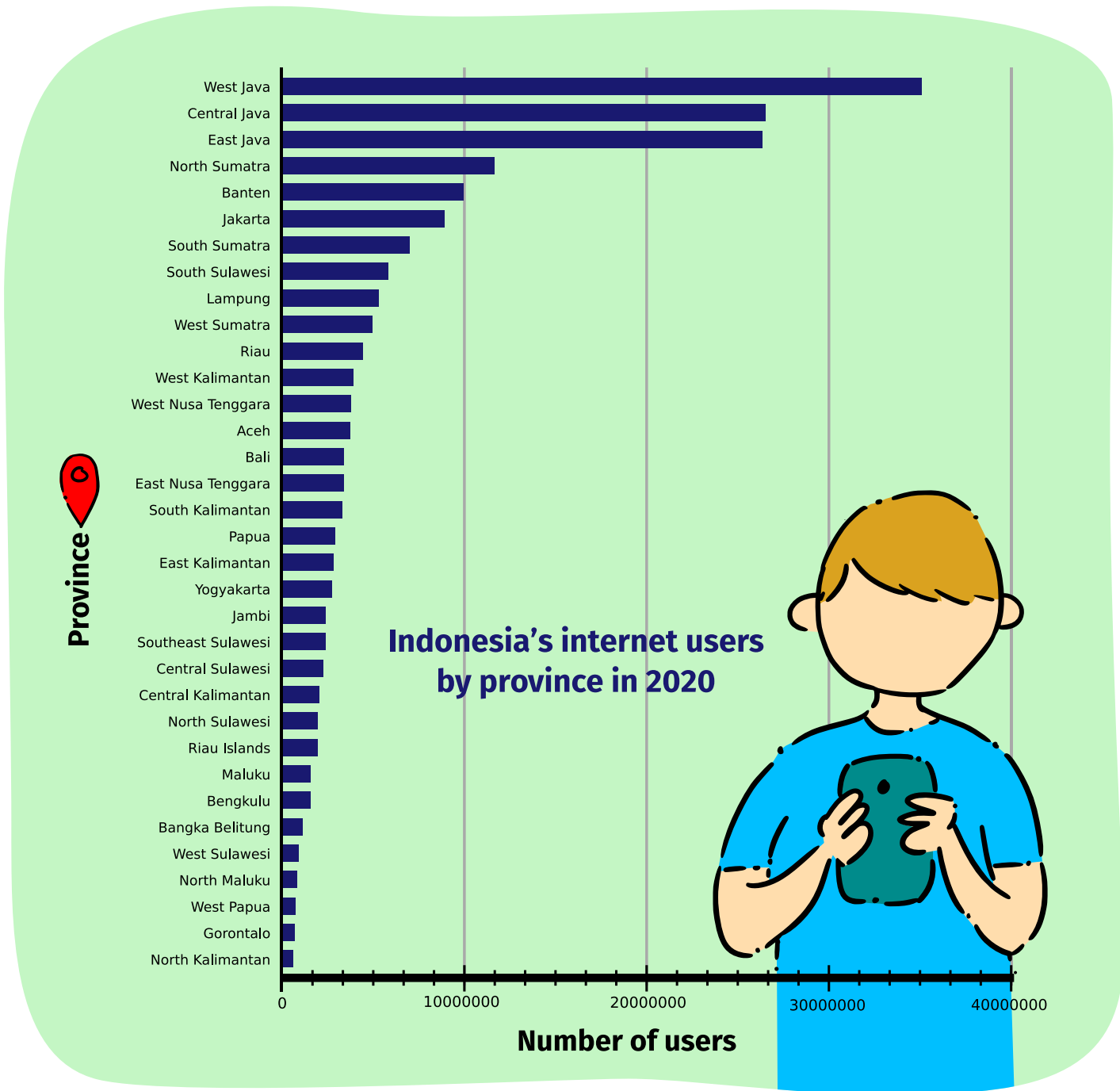


Figure 1. Indonesia's internet users by province in 2020  
Source: APJII (2020)

The inequality becomes even more jarring when the data are grouped by islands, with Java being home to the highest percentage of internet users at 56.4% of the island's total population while only 3% the population in Maluku and Papua are connected to the internet. This means that 56 out of 100 people in Java can access the Internet, while only 3 out of 100 people in Maluku and Papua do. The following illustration visualizes the wide gap in Internet access between islands in Indonesia.

Such wide gap in internet access poses a serious impact on Indonesia's digital divide. And four important factors can be attributed as causing this gap: infrastructure, skills, language content, and inefficient use of the Internet;<sup>3</sup> whereas unequal availability of hardware and software across different regions primarily contributing to infrastructure gap that disproportionately affect those in rural areas.

Meanwhile, low level of education is related to the other three factors. Re-

### Indonesia's internet users by islands in 2020

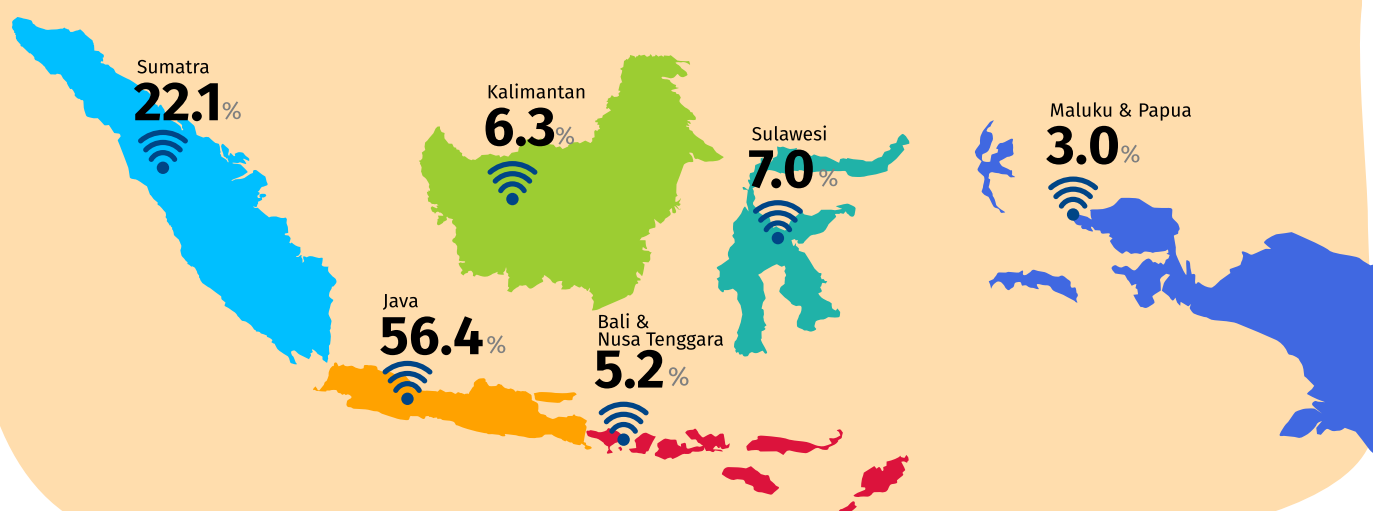


Figure 2. Indonesia's internet users by islands in 2020

Source: APJII (2020)

3 <https://media.neliti.com/media/publications/41183-ID-studi-pengukuran-digital-divide-di-indonesia.pdf>

latively low level of education leaves many with limited ability to operate a computer. And when they do have devices and are able access the internet, some face further difficulties due to language barriers. As a result, the internet is often used to access entertainment content more than to improve skills and knowledge. Combined with the infrastructure gap, low level of digital literacy continues to widen the digital divide.

### **Impact on Economic, Social, and Cultural Rights**

Restrictions caused by the COVID-19 pandemic have led to increased use of the internet, particularly for work, school, and social interactions. However, unequal access means that conducting those activities, which represent major aspects of our social, economic, and cultural rights, are not as easy for some as they are for others. As such, government policies, especially on education and economy, have also been impacted.

### **Education**

The Ministry of Education and Culture began implementing the distance learning program with the issuance of Ministerial Circular No. 15 of 2020. The circular states that distance learning is carried out by both online and offline, with the internet being the primary

means being used for online learning and television and radio broadcast, self-study modules, and others being used for offline learning.

Unfortunately, the policy overlooks the state of internet access and infrastructure across different communities. The Ministry's own data reported in July 2020 that 8,522 schools in Indonesia did not have access to electricity<sup>4</sup> and 42,159 schools did not have access to the internet. Three months later, the Ministry stated that, in fact, only 12,000 schools did not have internet access while about 48,000 schools are connected to the internet but with poor quality.<sup>5</sup> Most of these schools are located in underdeveloped rural areas.

In addition to infrastructure problems, many students cannot participate in distance learning because they do not have smartphones<sup>6</sup> or other devices to access the internet. Oftentimes, this is because many households own only one device which is also being used by the parents. The high cost of internet and technology devices—such as smartphones, tablets, laptops, and computers—has deprived many more Indonesian students of their basic right to education.

With all these difficulties, some students have reported higher level of

4 <https://news.detik.com/berita/d-5108489/kemendikbud-8522-sekolah-belum-berlistrik-42159-tak-ada-akses-Internet>

5 <https://www.cnnindonesia.com/nasional/20201022123707-20-561482/kemendikbud-12-ribu-sekolah-tak-punya-akses-Internet>

6 <https://tekno.tempo.co/read/1368691/tak-punya-smartphone-banyak-siswa-tak-ikut-pendidikan-jarak-jauh>



stress due to online learning resulting in more excessive assignments—in one case, the pressure even led to a student committing suicide.<sup>7</sup> Some students also find it harder to follow lessons and are at risk of dropping out. In other cases, students have also been reported to fall victims to criminal acts as they struggle to find stable internet connection.<sup>8 9</sup>

A survey conducted by the Indonesian Child Protection Commission (KPAI)<sup>10</sup> corroborates these reports. As many as 77.8% of student respondents expressed difficulties of participating in distance learning, with 37.1% feeling exhausted and stressed out due to time constraints, 42% unable to afford internet access, and 15.6% unable to afford the devices needed to access the internet. Similar finding was reported by a Saiful Mujani Research and Consulting (SMRC) survey with 92% of grade school and university students facing difficulties to take part in distance learning. A major cause is due to the absence of aid from the govern-

ment or schools in providing devices and internet connection, therefore leaving students to rely almost exclusively on their parents.<sup>11</sup>

In response, the government announced a "relaxation" policy<sup>12</sup>, which allows schools to use their operational grants (commonly referred to as BOS) to purchase internet data as well as adjust the curricula and staff teaching hours despite objections from the Parliament.

A swifter response instead came from the private sector instead, particularly telecommunication operators, who announced free internet data programs to several online learning sites.<sup>13</sup> However, this was still inadequate as it provided free access to certain sites only, whereas the students needed unrestricted free access to join video calls, virtual meetings, and chat messages. As a result, these free data often go to waste. Eventually, in August 2020, the government did announce a 9 trillion Indonesian rupiah (approximately

7 <https://www.liputan6.com/news/read/4388386/siswa-bunuh-diri-karena-tugas-daring-belajar-jarak-jauh-dinilai-perlu-evaluasi>

8 <https://www.medcom.id/pendidikan/news-pendidikan/PNgWARPn-siswa-di-ntt-naik-gunung-mencari-sinyal-demi-belajar-daring>

9 <https://www.msn.com/id-id/berita/dunia/siswi-smp-diperkosa-saat-belajar-daring-dan-mencari-sinyal-di-hutan/ar-BB1d1syq>

10 <https://nasional.tempo.co/read/1369405/empat-saran-kpai-untuk-pembelajaran-jarak-jauh-periode-kedua>

11 <https://lpmpdki.kemdikbud.go.id/survey-pelaksanaan-kebijakan-pendidikan-dalam-masa-darurat-penyebaran-coronavirus-disease-covid-19/>

12 <https://www.beritasatu.com/nasional/666959/kemdikbud-relaksasi-kebijakan-telah-dilakukan-selama-pjj>

13 <https://nasional.sindonews.com/read/143256/15/mewujudkan-merdeka-belajar-butuh-merdeka-jaringan-Internet-1598328509>

620 million US dollar) subsidy to cover the expenses of teachers, students, and lecturers on internet data.<sup>14</sup>

After all, in its implementation, the subsidy was also not without its own problems, mainly gaps in infrastructure and service coverage as well as moral hazard. For example, the subsidy was only available for customers of certain vendors, leaving those subscribed to different providers or outside the select vendors' service areas out of the subsidy program. Lack of accountability also remains a huge problem, exposing the subsidy program to mismanagement and abuse. Ultimately, the subsidy policy failed to address the real problems of unequal access to the internet and electricity.

### Economy

Limited Internet access also prevented some people from fulfilling their economic rights during the COVID-19 pandemic.<sup>15</sup> The Ministry of Cooperatives and Small and Medium Enterprises stated that 67,051 micro, small, and medium enterprises (MSMEs), or 90% of all MSMEs in Indonesia, were affected by the pandemic. Five business categories are affected the most: food

and beverages, wholesale and retail, processing industry, service industry, and the agriculture, forestry, and fisheries sector.<sup>16</sup>

Given these conditions, the Ministry have introduced the UMKM Go Digital program to help businesses enter the digital marketplace, targeting for at least 30 million out of 64 million MSMEs across the country to be integrated into the digital marketplace by 2023.<sup>17</sup> Before the pandemic, there were only around 8 million MSME to have been integrated. In 2020 alone, this number had increased by 3.7 million.

While promising, the implementation of the program is not without obstacles. Apart from limitations in terms of logistical and production capacity, costly and unstable internet access are some of the bigger challenges.<sup>18</sup> Unequal distribution of internet access is yet again a fundamental problem that the government has not been able to solve.

In turn, the government claims to be taking several actions, such as providing educational support and business training as well as providing mobile

<sup>14</sup> <https://nasional.sindonews.com/read/145556/15/akhirnya-pemerintah-alokasikan-rp9-triliun-untuk-pulsa-siswa-dan-guru-1598501293>

<sup>15</sup> <https://investor.id/business/kemenkop-ukm-90-umkm-terdampak-pandemi-covid19>

<sup>16</sup> <https://economy.okezone.com/read/2020/07/15/320/2246713/5-jenis-umkm-yang-paling-terdampak-covid-19>

<sup>17</sup> <https://www.cnnindonesia.com/ekonomi/20210111110041-92-592065/pemerintah-targetkan-30-juta-umkm-go-digital-pada-2023>

<sup>18</sup> <https://www.pikiran-rakyat.com/ekonomi/pr-01583669/diminta-go-digital-pelaku-umkm-keluhkan-mahalnya-akses-Internet>





*Children in the remote Air Baru Village, OKU Selatan, South Sumatra have to hike the hill in their hometown in order to be able to get internet reception to attend online classes due to inadequate internet infrastructure in November 2020.*

**Limited internet access for school students has resulted in a number of impacts, such as not being able to follow learning properly, being overwhelmed by a lot of learning tasks to stress and even suicide, as well as the threat of crime when searching for internet signals to mountains, forests, and places prone to crime.**

phone credit subsidies to help MSMEs access digital platforms.<sup>19</sup> However, the challenge with this type of subsidy programs remains the same as it is in the education sector, which is whether or not it goes to the right recipients. Data discrepancy across levels of government risks the program to bias in its distribution and could lead to confusion for the entrepreneurs.

Another economic challenge that surfaced during the pandemic is massive layoffs which resulted in many losing their source of income. Several sectors have been hit the hardest, particularly construction (making up 29.3% of recorded layoffs as well as wholesale, retail, restaurants, and accommodation services (28.9%). This is in line with the global data reported by the International Labor Organization (ILO) specifying the impact of the pandemic on four sectors: (1) wholesale, retail, and motor vehicle repair, (2) manufacturing, (3) accommodation and food industries, and (4) property and business management and administration services.<sup>20</sup>

The SMERU Research Institute found two implications of the economic crisis caused by the pandemic on the labor sector: an increase in the unemployment rate and changes in the post-crisis labor market landscape.<sup>21</sup> This is worsened by the fact that 26.1% of workers laid off during the pandemic were not awarded severance pay, according to research by the Population Research Center of the Indonesian Institute of Sciences (LIPI).<sup>22</sup>

Meanwhile, the government has been focused on rolling out and optimizing the impact of its Pre-Employment Card and social assistance programs. Compiling data from a variety of sources, we recorded that different regions give out different amounts of cash assistance, such as 600 thousand rupiah (approximately 40 US dollar) in Sidoarjo, East Java,<sup>23</sup> 2 million rupiah (approximately 138 US dollar) in Purwakarta, West Java,<sup>24</sup> and 2.5 million rupiah (approximately 170 US dollar) in Bogor, West Java.<sup>25</sup> Several communities and civil society organizations have also contributed cash assistance, such

19 <https://katadata.co.id/ekarina/berita/5efd920066212/pemerintah-dorong-umkm-gunakan-pembiayaan-murah-untuk-go-digital>

20 International Labor Organization (2020) *ILO Monitor: COVID-19 and the World of Work*, 3<sup>rd</sup> Edition.

21 <https://www.kompas.com/tren/read/2020/08/11/102500165/pandemi-covid-19-apa-saja-dampak-pada-sektor-kenagakerjaan-indonesia?page=all>

22 Ruth Meiliana, N. and Purba, Y. N. (2020) *Dampak Pandemi Covid-19 terhadap PHK dan Pendapatan Pekerja di Indonesia*. In *Jurnal Kependudukan Indonesia*, Edisi Khusus Demografi dan COVID-19, July, pp. 43–48.

23 <http://portal.sidoarjo.go.id/5000-korban-phk-terima-bantuan-sosial-dari-pemkab-sidoarjo-pj-bupati-hudiyono-ini-wujud-hadirnya-pemerintah>

24 <https://www.republika.co.id/berita/qidbsb423/korban-phk-di-purwakarta-dapat-bantuan-sosial-tunai>

25 <https://www.republika.co.id/berita/qiaexm366/warga-bogor-kena-phk-dapat-bantuan-rp-25-juta>



as the Indonesian Diaspora network who provided 700 thousand rupiah (approximately 48 US dollar) to those that had been laid off.<sup>26</sup>

Yet again, limited internet access has also become an obstacle in this instance. Enrollment in the Pre-Employment Card program, for example, requires filling out an online application on the Manpower Ministry's website. The so-called Pre-Employment Card itself does not come in physical but digital format.<sup>27</sup> Successful applicants are then selected on a first-come first-serve basis, a policy that is highly biased of the gap in class within the society, given that those with faster internet access and available resources could easily get into the program by the virtue of simply applying ahead of those with slower internet access and limited resources.

Digital literacy has also been an issue as there have been multiple fake Pre-Employment Card websites circulating, attempting to steal personal data of unsuspecting citizens. Lack of accountability and oversight in the application process means that it is also prone

to be misused by “jockeys” who apply on behalf of other people and then receive portions of the cash assistance as reward. Lastly, as the program provides online skill training on top of cash assistance, people with unreliable internet access must then face the next set of challenges, as attending these trainings mean they would need to purchase internet data and be in possession of the necessary resources to access the online sessions amid all the difficulties of the pandemic.

The pandemic did not create these new challenges. In truth, it simply exposed the recurring gaps that have already existed in Indonesia for a very long time. It simply taught us that internet access is not a luxury, but a fundamental right that is important for people in order to fulfill their economic, social, and cultural rights. Without adequate internet access, people who are already in vulnerable situations lose further as they are unable to fulfill their rights to an education and a decent livelihood. For minority groups such as Papuans and refugees in Indonesia, these situations place them in a dangerous position.

26 <https://www.cnbcindonesia.com/news/20200519193508-4-159669/anda-kena-phk-bisa-dapat-rp-780-ribu-bulan-nih>

27 <https://money.kompas.com/read/2019/11/20/210800226/ini-cara-mendapatkan-kartu-pra-kerja>



Picture: Suara Papua

*A resident of Jayawijaya, Papua held signs protesting bad internet access in their region.*

### Situation in Papua:

#### **Access shutdown and continued criminalization**

**T**he impact of the COVID-19 pandemic were felt not only in terms of public health, but also in the social and cultural aspects of the Papuan people's lives. Self-isolation order for those who tested positive for the disease, for example, removes an individual from the local culture of living communally among clans and family groups. This is exacerbated by the false stigma that COVID-19 is a type of AIDS, a curse, and so on—leading to a discriminatory attitude toward patients of the disease.

For those who try to obey government recommendations to observe self-quarantine and follow standard health protocols, that means conducting their activities online. But that is not easy since internet connection quality in Papua is notably poor compared to

other regions in Indonesia. It effectively hampers the circulation of important public health information regarding the COVID-19 pandemic, job opportunities, education, and civil expressions. Many students also find it difficult to enroll in schools, mainly because school and university websites cannot be accessed, such as the case in Wamena as well as other mountainous regions across Papua.

On 23 June 2020, more than 50 Papuans in Jayawijaya Regency held a demonstration at the Wamena office of Telkomsel and the Jayawijaya Local Representatives Council (DPRD). They demanded that the state-owned telecommunications company take immediate actions to improve its internet connection in the region.

As is with other regions in Indonesia, students in Papua experience similar difficulties with the distance learning policy, as many do not own smartpho-



nes or laptops to access online classes. In SMPN 3 Jayapura junior high school, students who do not have smartphones have no other options but to continue attending school in person. Other areas face an even bigger problem as they do not have access to electricity. In other areas, such as Paniai and Dogiyai, only 2G network connection is available, which is insufficient to attend online classes.

### Internet Shutdown

As if limited internet access was not enough, some Papuan civil activists have also experienced physical shutdown of internet access. Such incident happened to public defenders of the Human Rights Advocacy and Research Institute (ELSHAM) Papua who were acting as counsels for seven Papuan political prisoners put on trial at the Balikpapan District Court, East Kalimantan. As the COVID-19 pandemic broke out in mid-March 2020, the trial has been carried out online.

Director of ELSHAM Papua, Rev. Matheus Adadikam, arranged for the public defenders to attend the trial in their office as the internet connection there is more reliable. However, as the lawyers were about to present their defense, the internet was disconnected. Upon inspection, the staff found that their internet cable had been cut. To date, no perpetrator has been arrested.

Such disruption was not an isolated incident. Throughout the year, SAFEnet

received four different reports of alleged internet slowdowns in Papua. Amid escalation of armed conflicts escalation in Nduga, Papua on 15 July as well as in Maybrat, West Papua on 22 July, there were reports that internet and mobile phone signals had been shut down. The following month, on the anniversary of the 2019 massive protests against racism on 15 August, there were reports that the government intentionally slowed down internet speed in Papua.

On 7 October, internet network in Papua was interruption twice in the morning and then in the evening. Ahead of 1 December, designated as the Independence Day of Papua, internet access in Manokwari was reported to have slowed down for several days. Despite these reports, SAFEnet was not able to independently confirm whether the disruptions were deliberate due to a lack of equipment, tools, and resources needed to investigate.

Repression against activists and residents in Papua and West Papua who are critical of government policies both on responding to conflicts in the region as well as handling of the pandemic also occurred. This included excessive arrests using problematic articles of the ITE Law. Among others, activists arrested included Melianus Duwita in January as well as Alvoariani Reba (also known as Qvaria) and Angela Magay (also known as Angela Thomas) in April 2020.

Refugees in Indonesia:

## **Abandoned at Home, Disconnected in a Foreign Land**

**R**efugees and asylum seekers are among the most marginalized groups in Indonesia, including in terms of digital rights. The root of the problem lies in the issuance of Communications and Informatics Ministerial Regulation No. 12 of 2016 on prepaid SIM card registration. The regulation stated, among others, that SIM cards must be registered using ID card number for citizens and passport or stay permit number for non-citizens. Any unregistered SIM cards are automatically blocked from being used as of 30 April 2018.

Such policy certainly puts refugees and asylum seekers at odds given that they do not have any proper legal documentation to register SIM cards to use. As such, the policy effectively hinders all refugees and asylum seekers from being able to connect to mobile phone and internet connections at all.

### **Victims of Bad Policy**

As Indonesia still has not ratified the 1951 UN Convention on Refugees, it remains a transit and not a destination country for refugees who have fled their country due to conflicts, wars, or other life-threatening reasons. On their journey, most refugees do not carry identification such as passports or stay permits. The only thing they would have is a refugee card issued by the United Nations High Commissioner for Refugees (UNHCR), whereas those who are seeking asylum will only have the UNHCR identification once they are accepted as refugees. As of 2020, UNCHR records about 13,700 refugees in Indonesia.

Before the policy on prepaid SIM Card registration was introduced, refugees could still use local SIM cards to communicate, but that has since changed. According to the Indonesian Civil Society Association for Refugee Rights Protection (SUAKA), the regulation effectively robs refugees of the opportunity to get a local SIM card as they carry no legal identification.

SUAKA Public Awareness and Campaign Coordinator, Zico Pestalozzi, said that his party had tried to register a prepaid card using the UNHCR card number. Even though the registration was successful, the operator then canceled it because the registration process was not in line with their procedure. In turn, many refugees resort to “borrowing” other people’s identification to activate a SIM card, with their landlords being the most common to help. They have also received help from SIM card vendors by paying additional amount of money to get help with the registration.

“When unregistered, the number will automatically be disconnected. Many refugees in Bogor are worried that communication with their family and friends back home and elsewhere would no longer be possible,” said Zico during an interview with SAFEnet.

While there are ways to go around the restrictions, the Ministerial Regulation renders many disconnected as not all would have local acquaintances to help them get a SIM card. As a result,

refugees are deprived of their digital rights. This, according to Zico, could instead exacerbate the situation with refugees in the country. This is because refugees without internet access tend to seek help and rely on others who do have internet access. Zico added that even without the regulation, refugees have already been exposed to many difficulties in terms of communication given their legal status. Imposing the regulation on SIM card registration on refugees, therefore, means that they will be deprived of their right to access the internet and the information that comes with it.

### **Robbed of Digital Rights**

While access to SIM cards is blocked, internet access is pivotal to the survival of refugees in Indonesia. According to SUAKA, there are at least three important functions of the internet for refugees: (1) to communicate with their family back home, (2) to obtain information that could impact their well-being, such as resettlement in their country of destination, updates of their homeland, and news of refugees in Indonesia, and (3) to receive education, especially during the COVID-19 pandemic, which has made it impossible for community learning centers for refugees to conduct in-person sessions, meaning that they too have had to use online application such as Zoom, Google Classroom, or WhatsApp.

Given the pandemic, refugees in general are also greatly affected as not all of them have internet access at home,

which they rent from locals. As such, they have to either find somewhere else to get internet connection or request their landlords to install internet service at their homes—effectively increasing their already limited living cost.

Additionally, since many refugees are not able to speak Indonesian, they often miss out on news and updates regarding the handling and prevention of COVID-19. Meanwhile, access to pandemic information in their native language is extremely limited. An effective alternative is to browse for these information online, but that would require access to the internet, which has become a luxury for them.

Internet access is also urgently needed by refugees to keep track of the UNCHR monitoring and assistance process. According to Zico, refugees should at least have a phone number for the UNHCR to contact. As refugees are not able to do so following the Ministerial Regulation, UNHCR has found it difficult to maintain communications, particularly with independent refugees or those who live in temporary, shelters where there is little to no coordination.

In light of these hardships, Zico emphasizes the need for an exception to the SIM card registration policy for refugees. They could, for example, use the identification on their UNHCR cards to obtain access to SIM cards or other internet services. Doing so could be beneficial for monitoring purposes and fulfill the digital rights of the refugees.



## Freedom of Expression

**W**hile the COVID-19 pandemic has put a pause on many human activities, particularly where large gatherings are involved, it has not been able to stop the continued criminalization against internet users in Indonesia. Throughout 2020, the number of legal actions taken against internet users have instead increased considerably.

Criminalization using problematic articles of the ITE Law in 2020 cannot be separated from the COVID-19 pandemic itself. In many cases, the victims are citizens who are critical of the government handling of the pandemic or those accused of spreading false information regarding COVID-19.

WP, who lives in Riau Islands, is one of those people who has fallen victim to criminalization over his online expression. On his personal Facebook account, WP uploaded a meme with a

picture of President Joko Widodo (Jokowi), captioning it "We will be watching if you corrupt the COVID-19 fund." According to him, it was only intended as a joke and, at the same time, a playful reminder for the government to handle the pandemic seriously.

However, not long after, WP was abruptly arrested by police officers on 8 April. He was accused of committing hate speech and insulting President Jokowi. He was subsequently charged with Article 28 (2) of the ITE Law on hate speech and face up to six years in prison.<sup>28</sup>

AS, who lives in Semarang, Central Java, experienced something eerily similar. Police officers arrested him on 20 April following a social media post that criticized the Semarang City Government's road closure policy intended to minimize mobility during the pandemic. In his comment, AS wrote "Is this for real, such a stupid regulation. I understand we are all afraid of the Corona[virus], but not like this. Everything is blocked. Whoever made this policy is so dumb."<sup>29</sup>

What WP and AS experienced are just a couple of examples to showcase how excessive criminalization against freedom of expressions have been during the pandemic. Throughout 2020, SAFEnet recorded at least 84 criminal cases against citizens for their expressions, almost four times the 24 cases recorded in 2019.

The ITE Law remains a looming threat against freedom of expression. Of the 84 cases recorded, 64 were processed using problematic, "catch-all" articles of the ITE Law, such as Article 28 (2) on hate speech which were cited in 27 cases, including WP's alleged hate speech against President Jokowi through a meme.

Article 27 (3) on defamation was the second most frequently cited, found in 22 cases. This included the case against a Facebook user by the name of Qvarica, who posted an opinion regarding the closure of Rendani Airport in Manokwari in April 2020. The account was subsequently reported by the legal team of the West Papuan Provincial Government, alleging that the user has insulted the West Papuan

28 [https://www.cnnindonesia.com/nasional/20200408192303-12-491818/diduga-hina-jokowi-soal-corona-buruh-di-kepri-ditangkap?utm\\_source=twitter&utm\\_medium=oa&utm\\_content=cnnindonesia&utm\\_campaign=cmsocmed](https://www.cnnindonesia.com/nasional/20200408192303-12-491818/diduga-hina-jokowi-soal-corona-buruh-di-kepri-ditangkap?utm_source=twitter&utm_medium=oa&utm_content=cnnindonesia&utm_campaign=cmsocmed)

29 <https://www.rmoljateng.com/read/2020/04/20/26730/Maki-Pemerintah-Soal-Penutupan-Jalan,-Pemuda-Ini-Ditangkap-Polisi-https://radarsemarang.jawapos.com/berita/semarang/2020/04/21/hina-pemkot-dimedsos-pemuda-gisikdrone-diciduk/>



Governor through their social media post.

Meanwhile, Article 28 (1) on consumer loss due to false information was cited in 12 cases. It is often used to arrest citizens on the pretext of preventing the spread of hoaxes and false information regarding COVID-19 and its handling by

the government. It was used, for example, in the case of Arina Maghfiroh, who lives in Ketapang, West Kalimantan. After uploading information of a Coronavirus patient being treated at the Agoesdjam Ketapang General Hospital on 4 March 2020, she was charged by local law enforcement with Article 28 (1) of the ITE Law.

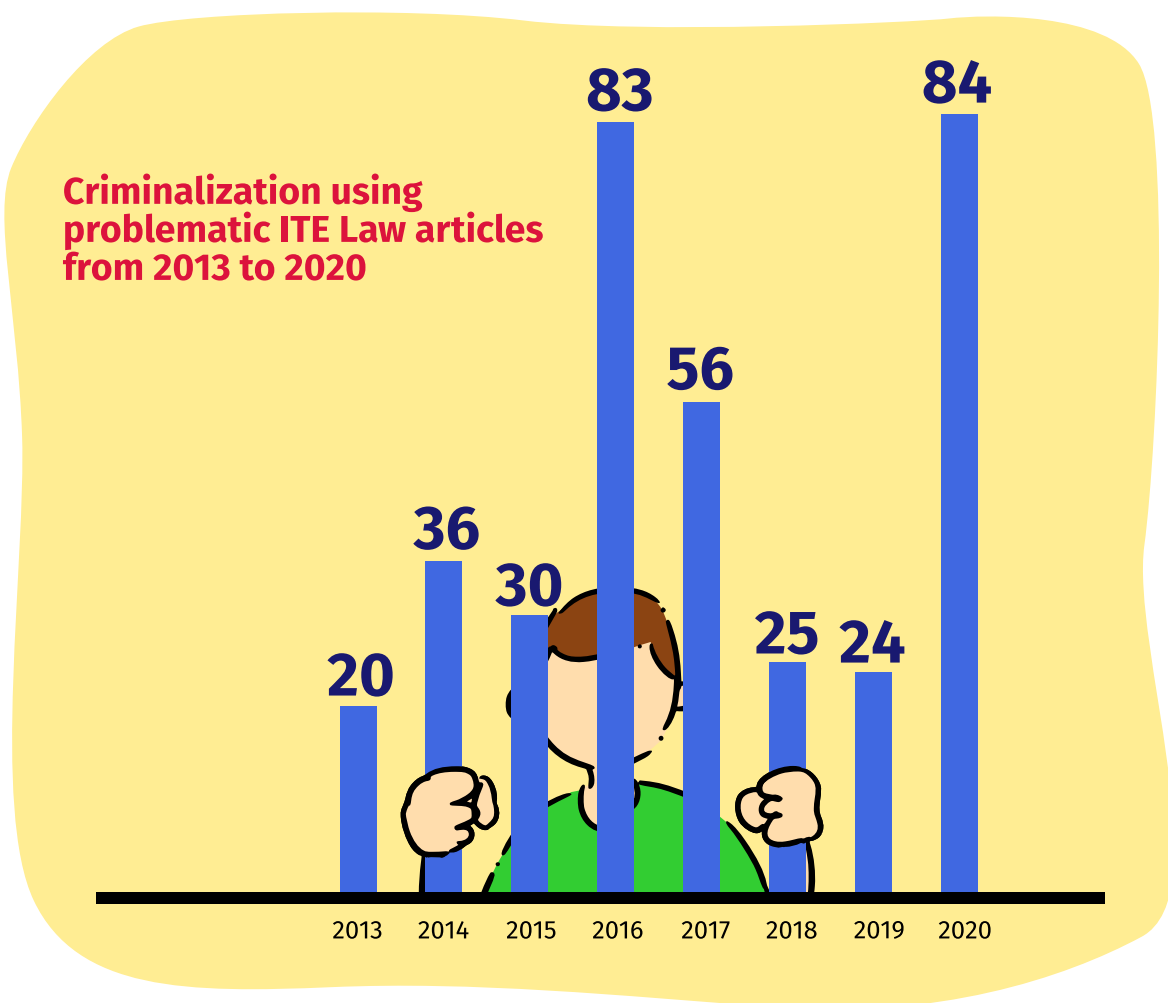


Figure 3: Number of criminalization to internet users in Indonesia (2013-2020)

In addition to the ITE Law, SAFEnet also observed a trend of using other problematic regulations to limit freedom of expression in the digital space. Arti-

cles 14–15 of Law No. 1 of 1946 on riots were cited in 21 cases as well as Articles 207 and 310 of the Criminal Code on insult and defamation.

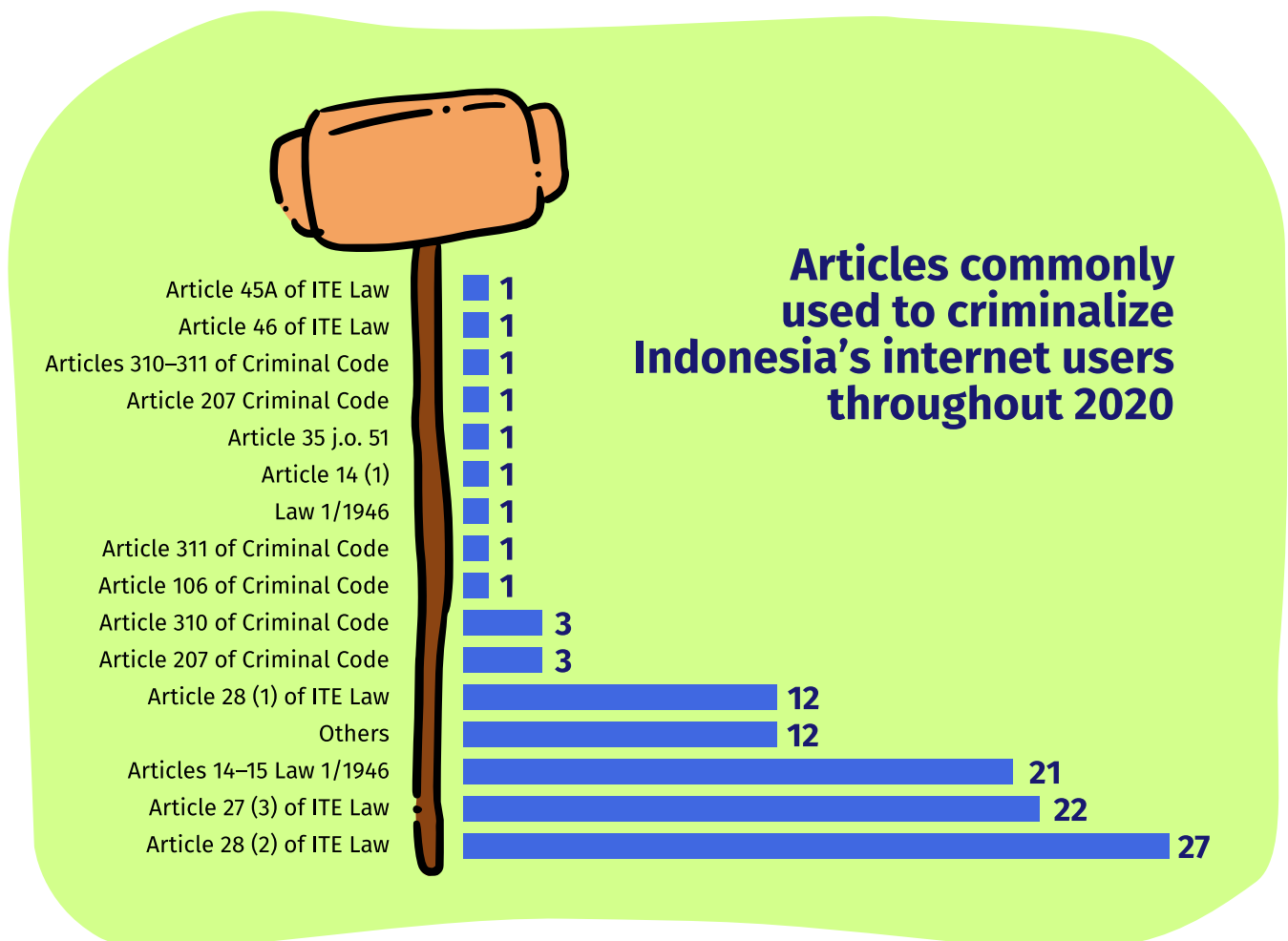


Figure 4. Articles commonly used to criminalize Indonesia's internet users throughout 2020

Among all the victims, regular citizens make up the biggest portion with 50 people, followed by social and political activists (15 people), labors (4), university students (4), private workers (3), grade school students (2), and journalist (1). By locations, the cases mostly took place in Java (43 cases), followed by Sumatra (11), Sulawesi (8), Kaliman-

tan (6), Nusa Tenggara (5), Bali (4), and Maluku (3).

Overall, the number of citizens and activists reported in 2020 was much higher than in 2019, when journalists were the most common victims with 8 cases, activists (5), and regular citizens (4).

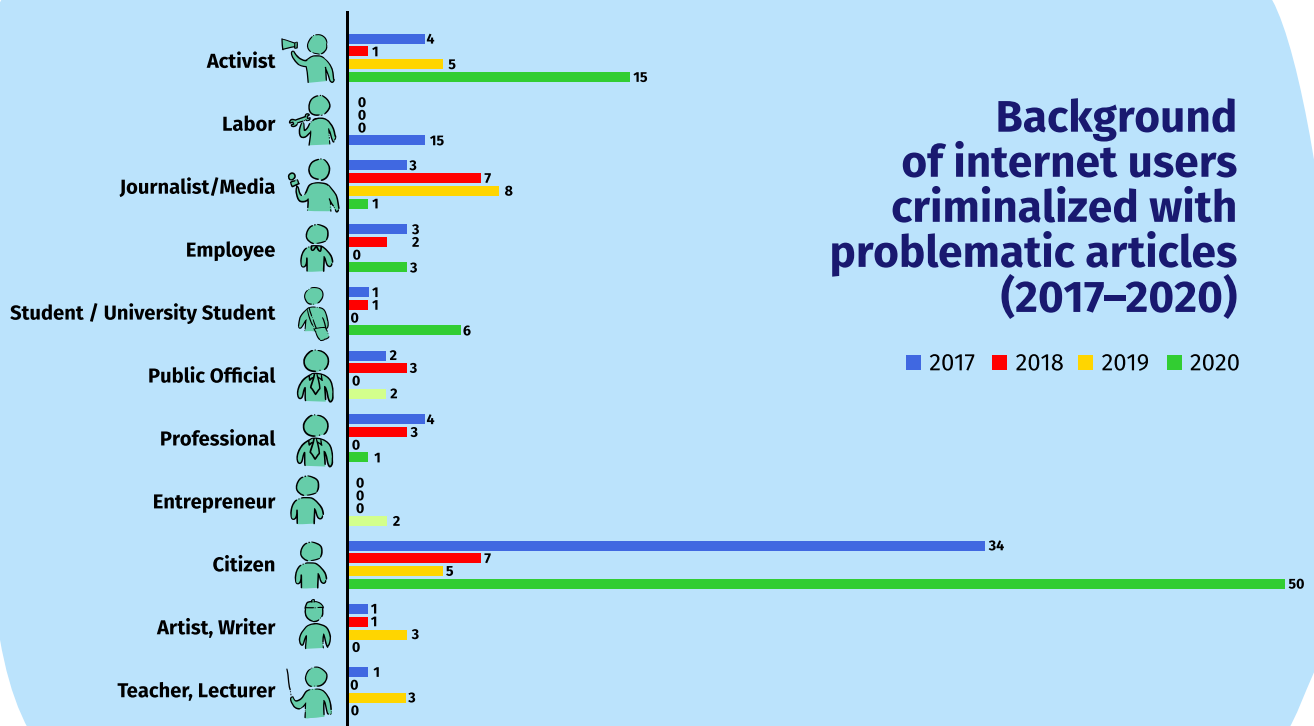


Figure 5. Backgrounds of internet users criminalized with problematic articles (2017-2020)

The increase in criminal charges brought against citizens during the pandemic can also be inferred from the data on the Police Force's cyber patrol website.<sup>30</sup> In 2020 alone, complaints of negative online content through the cyber patrol categorized as insults and defamation dominated with 1,477 complaints, followed by pro-

vocations with 172 complaints, and religious blasphemy with 96 complaints. Meanwhile, despite fewer number of police reports made regarding provocative online content in 2020 with 1,048 reports, down from 1,769 reports in 2019, it still marks a 7% increase in terms of proportion to overall reports, from 38.5% in 2019 to 46.3% to 2020.

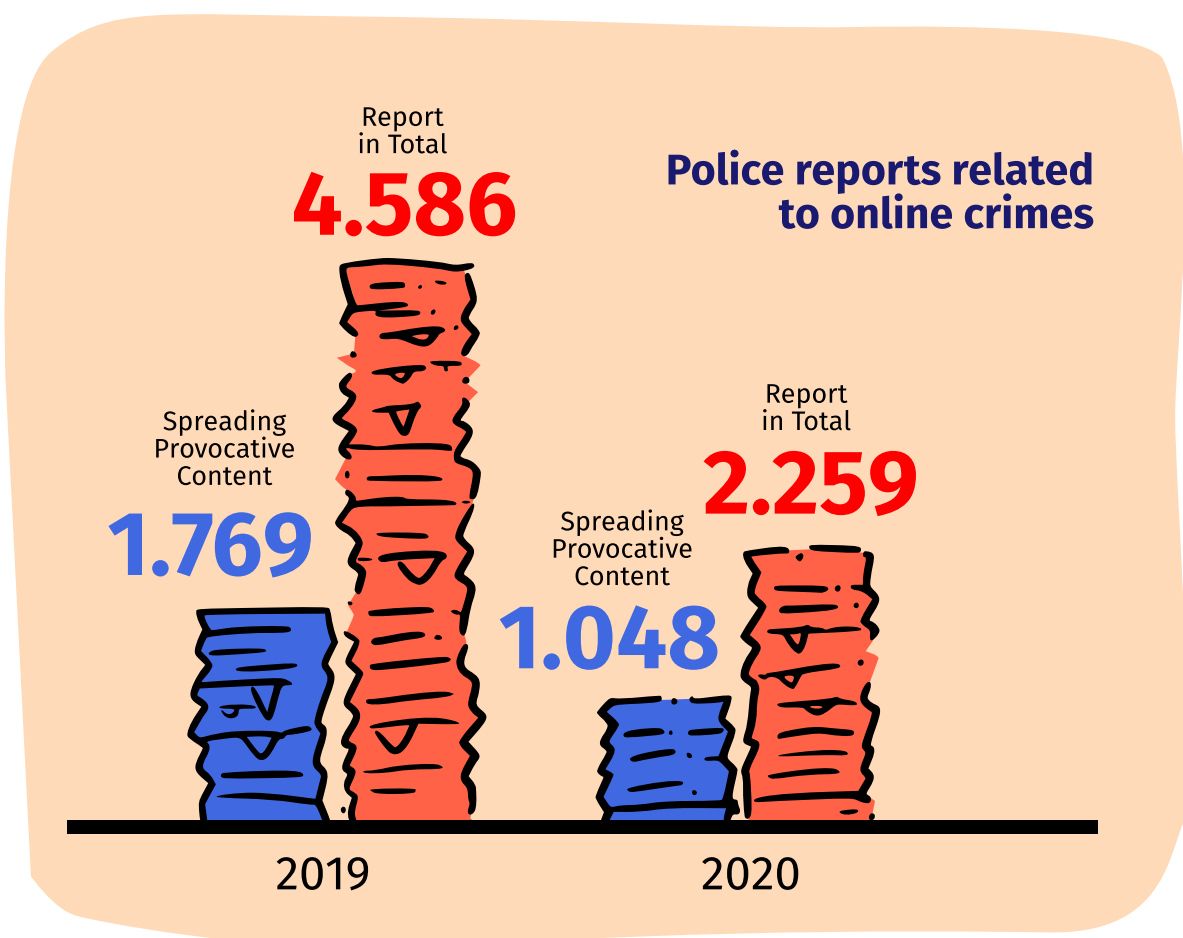


Figure 6. Police reports related to online crimes (2019–2020)  
Source: Cyber Patrol

<sup>30</sup> <https://patrolisiber.id/home>

The Supreme Court also noted that the number of convictions on particular criminal cases related to the ITE Law in 2020 reached 690 convictions, an increase from the 670 convictions recorded in 2019 and the highest since 2017.

### Telegrams to Silence

The rise in convictions against netizens could be observed to have occurred following the publication of two Natio-

nal Police Chief telegrams. The first one, ST/1100/IV/HUK.7.1.2020, came on 4 April with the instruction his to carry out cyber patrols to news opinion circulating online, particularly targeting hoaxes regarding COVID-19 and government policies in dealing with the outbreak as well as insults against the president and other government officials.

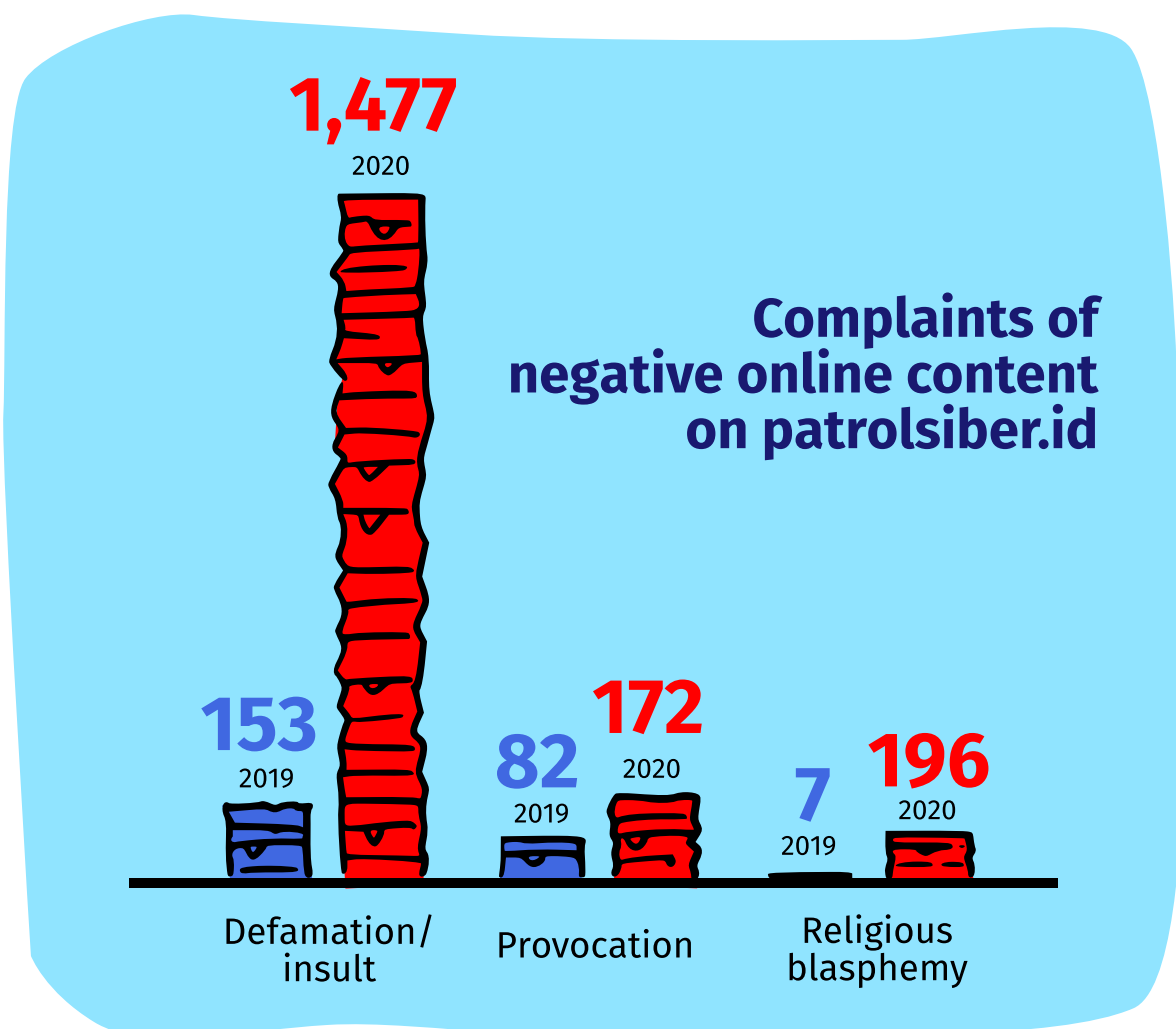


Figure 7: Negative content report through patrolsiber.id  
Source: Patroli Siber

KEPOLISIAN NEGARA REPUBLIK INDONESIA  
MARKAS BESAR



SURAT TELEGRAM

DARI : KAPOLRI

DERAJAT : KILAT  
KLASIFIKASI : RHS

KEPADA : PARA KAPOLDA

TEMBUSAN: 1. KAPOLRI  
2. WAKAPOLRI  
3. IRWASUM POLRI  
4. PARA KABA POLRI  
5. PARA ASISTEN KAPOLRI  
6. KADIVHUMAS POLRI  
7. DANKORBRIMOB POLRI

NOMOR: STR/ 645 /X/PAM.3.2./2020

TGL 2 - 10 - 2020

AAA TTK REF TTK DUA

SATU TTK UU NOMOR 2 TAHUN 2002 TTG POLRI TTK

DUA TTK RENKON AMAN NUSA I NOMOR: R/RENKON/1/OPS.2./2020 TGL 1 JANUARI 2020 TTG MENGHADAPI KONTINUENSI KONFLIK SOSIAL TAHUN 2020 TTK

TIGA TTK KIRKAT BAINTELKAM POLRI NOMOR: KIRKAT-491/VI/IPP1.3./2020/BIROANALIS BULAN JUNI 2020 TTG REN PEMBAHASAN OMNIBUS LAW RUU CIPTA KERJA YANG BERPOTENSI MENIMBULKAN AKSI PENOLAKAN TTK

EMPT TTK VIDCON HARI KAMIS TANGGAL 1 OKT 2020 TTG RAKOR WAKAPOLRI DAN MENTERI KETENAGAKERJAAN TTK

BBB TTK SEHUB DGN REF TSB DI ATAS KMA DIINFORMASIKAN KPD KA BAHWA UPDATE TERKINI PEMBAHASAN RUU OMNIBUS - CIPTA KERJA KMA MASIH MENDAPAT PENOLAKAN DARI BBRP ELEMEN BURUH DAN MASY SERTA ADANYA ISU UNRAS DAN MOGOK KERJA YG AKAN BERPOTENSI BERDAMPAK PD KESEHATAN KMA EKONOMI KMA MORAL DAN HUKUM TTK

CCC TTK BERKAITAN DGN POIN AAA DAN BBB KMA DLM RANGKA MENJAGA SITKAMTIBMAS YG KONDUSIF SERTA ANTISIPASI AKSI UNRAS DAN MOGOK KERJA YG AKAN DILAKUKAN OLEH BURUH PADA TGL 6 - 8 OKT 2020 BERKAITAN DENGAN PENOLAKAN RUU OMNIBUS LAW - CIPTA KERJA DITENGAH PANDEMI COVID-19 KMA AGAR KA MELAKUKAN LANGKAH-LANGKAH SBB TTK DUA

SATU TTK .....

Digambar dengan CorelDraw

*National Police Chief telegram in anticipation of the Jobs Creation Omnibus Law issued in October 2020 (Source: National Police Chief Telegram)*



- SATU TTK MELAKSANAKAN GIAT FUNGSI INTELJEN DAN DETEKSI DINI SERTA DETEKSI AKSI TERHADAP ELEMEN BURUH DAN MASY GUNA MENCEGAH TERJADINYA AKSI UNRAS DAN MOGOK KERJA YG DAPAT MENIMBULKAN AKSI ANARKIS DAN KONFLIK SOSIAL DI WILAYAH Masing-Masing TTK
- DUA TTK MAPPING PERUSAHAAN/SENTRA PRODUKSI STRATEGIS DIWILAYAH Masing-Masing DAN BERIKAN JAMINAN KEAMANAN DARI ANCAMAN/PROVOKASI YG MEMAKSA IKUT UNRAS DAN MOGOK KERJA TTK
- TIGA TTK CEGAH KMA REDAM DAN ALIHKAN AKSI UNRAS YG DILAKUKAN POK BURUH MAUPUN ELEMEN ALIANSINYA GUNA MENCEGAH PENYEBARAN COVID-19 TTK
- EMPT TTK MELAKUKAN KOORDINASI DAN BANGUN KOMUNIKASI YG EFEKTIF DGN APINDO KMA DISNAKER KMA TOKOH BURUH KMA MAHASISWA DAN ELEMEN MASY LAINNYA DLM RANGKA MEMELIHARA SITKAMTIBMAS KONDUSIF DITENGAH PANDEMI COVID-19 TTK
- LIMA TTK LAKUKAN CYBER PATROL PADA MEDSOS DAN MANAJEMEN MEDIA UTK BANGUN OPINI PUBLIK YG TDK SETUJU DGN AKSI UNRAS DI TENGAH PADEMI COVID-19 TTK
- ENAM TTK LAKUKAN KONTRA NARASI ISU-ISU YG MENDISKREDITKAN PEMERINTAH TTK
- TUJUH TTK SECARA TEGAS TDK MEMBERIKAN IZIN KEGIATAN BAIK UNJUK RASA MAUPUN IZIN KERAMAIAAN LAINNYA TTK
- DLPN TTK UPAYA HARUS DILAKUKAN DI HULU (TITIK AWAL SEBELUM KUMPUL) KMA DAN LAKUKAN PAM TERBUKA DAN TERTUTUP TTK
- SBLN TTK JGN LAKUKAN PENCEGATAN DI JALAN TOL KARENA DPT BERJIMBAS PENUTUPAN JALAN TOL YG DAPAT MENJADI ISU NASIONAL DAN INTERNASIONAL (INI JUSTRU YG MEREKA KEHENDAKI) TTK
- SPLH TTK LAKUKAN GAKKUM TERHADAP GAR PIDANA KMA GUNAKAN PASAL-PASAL KUHP KMA UU KEKARANTINAAN KESEHATAN KMA DLL TTK
- SBLS TTK SIAPKAN RENPAM UNRAS DENGAN TETAP MEMPEDOMANI PERKAP NO 16 TAHUN 2006 TTG PENGENDALIAN MASSA KMA PERKAP NO 1 TAHUN 2009 TTG PENGGUNAAN KEKUATAN DALAM TINDAKAN KEPOLISIAN DAN PROTAP NO 1 TAHUN 2010 TTG PENANGGULANGAN ANARKIS TTK

DBLS TTK .....

Digndai dengan Carellesonee

The second one, STR/645/X/PAM.3.2./2020, came on 2 October amid massive public criticism and protest against the passing of the Jobs Creation Omnibus Law. It instructs police officers to conduct further cyber patrols on social media and build media sentiment denouncing the demonstrations against the controversial amid the pandemic as well as orders to spread counter-narratives to issues that are perceived as discrediting the government.

The two telegrams are problematic because they could be seen as encouraging repression and abuse of authorities by police and the law enforcement. They are also prone to triggering violations of freedom of expression as they include points on criminalizing opinions deemed as insults against the president and other government officials. In its implementation, as suggested by the available data, the telegrams allow the law enforcement to criminalize public opinions and criticisms.

The high criminalization rate has inevitably created a greater climate of fear. A National Human Rights Commission survey in December 2020 involving 1,200 respondents indicated that 29% expressed fear of voicing criticisms toward the government and 36.2% were particularly fearful of voicing criti-

cisms on social media and the internet.

These circumstances have rather been ironic as people are becoming more dependent on the internet to communicate and express their opinions given the COVID-19 pandemic and the recommendation to stay home. APJII noted a 20% to 25% surge in data traffic during the implementation of large-scale social restrictions in the first six months of the pandemic,<sup>31</sup> which means that the use of internet to express opinions and distributing information has also seen a considerable increase.

Unfortunately, the pandemic is also being used by the law enforcement in Indonesia to exert excessive restrictions on free expression, particularly by using the ITE Law and other problematic regulations. The high criminalization rate also negates the objective of the government's policy of granting early release for low-level prisoners to prevent the transmission of COVID-19 in prisons.

Freedom of expression is one of the fundamental component of a democratic society as well as an important prerequisite for the advancement of a society. It is also pivotal in ensuring the fulfillment of human rights and other fundamental freedoms. The go-

31 <https://teknologi.bisnis.com/read/20200813/101/1278818/pandemi-covid-19-dorong-kenaikan-trafik-data-hingga-25-%>

vernment, therefore, should have refrained from intervening and limiting the freedom of expression and instead provides full protection for everyone to freely express themselves.

As Article 19 (2) of the International Covenant on Civil and Political Rights (ICCPR), passed in 1966, states: "Everyone has the right to freedom of expression; this right includes freedom to seek, receive, and impart any information and thoughts, regardless of limitations orally, in writing, or in printed form, artwork, or through other means of his/her choice."

### **Repression on the Pretext of Misinformation and Disinformation**

Next to insulting the president and other government officials, one of the most common pretext for the criminalization of during the pandemic has been accusations of spreading misinformation and disinformation. Based on the National Police Cyber Crime data, the number of police reports related to fake news or hoaxes has continued to increase over the years, from 60 in 2018, 97 in 2019, and 197 in 2020.

SAFEnet analysis results show that there are two typologies of content often targeted for criminalization: hoax

and false information and criticisms labeled as hoax by the law enforcement officials.

In reality, hoax can be classified into three different types: misinformation, disinformation, and malinformation. Misinformation occurs when false information does not cause harm and is often unintentional. Disinformation, on the other hand, occurs when false information is deliberately created to cause harm. Meanwhile, malinformation occurs when the information is based on actual facts but is being used to deliberately cause harm.<sup>32</sup>

Article 28 (1) of the ITE Law regulates that the spread of fake news on electronic media, which includes social media, as "Everyone knowingly, and without right, spreads false and misleading news that results in consumer losses in Electronic Transactions." Violation of this article is subject to maximum imprisonment of 6 years and/or a fine up to 1 billion rupiah (approximately 70 thousand US dollar). Meanwhile, the Indonesian Main Dictionary interprets hoax as simply "fake news". Given that Article 28 (1) does not offer any characterization or clear definition of fake news, its implementation has therefore been widely considered as problematic. In reality, the intention of

<sup>32</sup> <https://en.unesco.org/fightfakenews>

this Article is actually to regulate fake news that cause consumer losses in electronic transactions.

IZ, a woman who lives in Blitar, East Java, was reported to the police using Article 28 (1) for a social media post which reads: "Instructions from the Regent of Blitar today. Blitar has been hit by the Corona outbreak. Infections have spread to the areas of Wlingi, Ponggok, Udanawu, Nglegok, Selopuro, and Gandusari areas. One patient from the Nglegok area has been transferred to Malang." The post, as it is, does not contain any information that could result in consumer losses in electronic transactions.

SA, who lives in Lombok, had a similar experience when he was cited by the police using the same article over his social media post which reads: "The Coronavirus has been detected in the Montong Gamang Village, Kopang District, Central Lombok."

In addition to Article 28 (1), content accused of being fake news has also been charged with Articles 27 (3) and 28 (2) of the ITE Law. This indicates that the law enforcement is also not entirely clear on the legal implementation of the articles regarding fake news itself and is therefore prone to abuse of

power in order to silence opinions.

SAFEnet considers that a legal approach to the spread of hoaxes is not the best option because the prevalence of hoaxes is related to multiple factors, from low digital literacy, platform algorithms, and social polarization. The advent of the internet has changed the flow of information, from monopoly by mass media organizations to user-generated content. Meanwhile, many are not equipped with the ability to distinguish facts from hoaxes.

The Communications and Informatics Ministry rated Indonesia's digital literacy in 2020 as moderate. In their report, 20.3% of respondents surveyed trust social media as the most reliable source of information, significantly higher than trust in online media at 7%.<sup>33</sup>

At a time when public health and livelihood of its people are at great risks, countries should not take advantage of the spread of fake news and crisis fueled by COVID-19 as an excuse to suppress criticisms in the digital space. The best approach to combat misinformation and disinformation should be to ensure public access to evidence-based and reliable information, not by putting people in prison for spea-

<sup>33</sup> Ministry of Communications and Informatics and KataData Insight Center (2020) *Status Literasi Digital Indonesia 2020: Hasil Survei di 34 Provinsi*.

king their minds on social media.

Meanwhile, SAFEnet has observed that the labeling of criticisms as fake news by law enforcement began to occur in 2019, most notably during the Papuan unrest following racist incidents which led to criminal actions being taken against human rights activist Veronica Koman and journalist Dandhy Laksono,<sup>34</sup> who was even further victimized by arbitrary arrest using the law enforcement's go-to problematic articles of the ITE Law.

The same pattern could be observed during the widespread public protest against the Jobs Creation Omnibus Law, which received massive criticisms as the legislation process did not involve the public and contained a number of articles perceived as threats toward labor welfare and environmental protection. Following its passing at the Parliament on 5 October 2020, multiple groups across the country began holding big demonstrations with massive criticisms being voiced online as well.

Amid the controversy, VE, a Twitter user, began distributing a digital poster highlighting 12 points included in

the Jobs Creation Omnibus Law considered as a threat toward labor welfare. Upon the post going viral, V was arrested by the police, and the post taken down as it was labeled as a hoax.<sup>35</sup> Additionally, nine senior activists who were affiliated with the Coalition of Action to Save Indonesia (KAMI) were also accused for spreading hoaxes after voicing criticisms toward the Jobs Creation Omnibus Law.<sup>36</sup>

All of these instances show that the pretext of misinformation and disinformation are being exploited by the government and law enforcement to silence critical voices. If continued, such practice could lead to the government monopolizing information and truth.

### **New Threat: Ministerial Regulation No. 5 of 2020**

On 16 November 2020, the Ministry of Communication and Informatics issued Regulation No. 5 of 2020 on Private Electronic System Operators, making Indonesia one of only a few governments to force social media platforms, online applications, and other online service providers to be liable to local jurisdiction over their content and user data policies and practices. If not pro-

34 Southeast Asia Freedom of Expression Network (2020) *Laporan Situasi Hak-Hak Digital Indonesia 2019: Bangkitnya Otoritarian Digital*.

35 <https://news.detik.com/berita/d-5208145/sebar-hoax-omnibus-law-pemilik-akun-videlyae-ditahan-bareskrim>

36 <https://www.cnnindonesia.com/nasional/20201015180344-12-558904/peran-9-anggota-kami-tersangka-uu-ite-penghasutan-ciptaker>





Picture: Diananta Putra's File

*Diananta Putra, Chief Editor of Banjahits.com, was one of a few journalists criminalized using the ITE Law in 2020.*

perly anticipated, this could potentially exacerbate government repression on freedom of expression.

This regulation does not only worsen the situation of freedom of expression in Indonesia, but also has the potential to be used as a justification of further human rights violations. SAFEnet analysis indicates that it allows the Ministry of Communication and Informatics excessive authority to assess and determine whether certain content is appropriate or not for circulation, opening a loophole to be used in silencing critical voices.

The excessive authority of the Ministry could be seen in multiple aspects,

from requiring electronic system operators to go through a registration process to exerting control over the content published on their platforms. The regulation requires every private electronic system operator to register and obtain an ID certificate issued by the Ministry in order to be able to operate in Indonesia and begin publishing content.

Setting a mid-May 2021 deadline, the regulation threatens that all operators will be blocked upon failure to comply. This constitutes not just an infringement of freedom of expression, but also of the International Covenant on Civil and Political Rights, which states that “nothing in this Covenant can be

construed as implying for any State [...] any right to be involved in any activity or taking any action aimed at destroying the rights and freedoms recognized in the present Covenant."

The regulation, signed by Communications and Informatics Minister Johnny Gerard Plate, also forces every individual whose digital content is used or accessed in Indonesia to appoint a local representative based in the country. While an argument could be made that this regulation is a step toward adjusting the rules to local content, the point on local representation will make it more difficult for operators to refuse arbitrary intervention and orders from the government and leave them vulnerable to domestic legal actions, including arrest and criminalization.

Furthermore, some articles in the regulation are also at risk of becoming problematic, catch-all articles as can be seen with the ITE Law. For example, Article 13 forces all private electronic system operators to remove all prohibited information and/or documents, which is defined in Article 9 (3) as information and content that violates the provision of Indonesian laws and regulations or creates "public unrest" or "disturbance to public order". Article 9 (4) gives the Ministry, which a non-independent authority, unfettered discretion to freely define what constitutes a "public unrest" or "disturbance to public order". It also forces operators to remove anything that could "inform

how to or grant access" to prohibited documents.

This situation is extremely concerning. SAFEnet argues that forcing operators to ensure that they do not "inform how to" or "grant access" to prohibited documents and information means that if operators or their users publish a guide, for example, on how to access prohibited information or content (such as by explaining how to use a VPN), then the guide itself could then be considered as prohibited information.

The regulation also authorizes a "Minister in charge of access blocking" to coordinate the blocking of prohibited information based on requests that could come from law enforcement agencies, courts, the Ministry of Communications and Informatics, or any members of the public. Courts can issue "instructions" to the Minister in charge of access blocking to, while the other parties can send requests for the Minister to review.

Once the Minister approves a request, they will then send an email to private electronic system operators with orders to block certain information within 24 hours—or 4 hours for "urgent" requests, which could include terrorism, child pornography, or content that causes "situations of public unrest and disturbance to public order".

The regulation also gives the Ministry to force internet service providers to block access to any private electronic

system and/or to impose fines that will accumulate every 24 or 4 hours based on its category up to 3 times (i.e. for urgent requests, the maximum fine will be imposed after 12 hours, while it takes 72 hours for regular requests to result in maximum fine). If operators fail to comply after 12 or 72 hours, Article 16 (11) and (12) rule that access to their electronic system will be blocked.

The implementation of this Communications and Informatics Ministerial Regulation will certainly worsen the situation of Indonesia's digital rights. As such, SAFEnet urges the Ministry to revoke the regulation as it is incompatible with international standards and laws on freedom of expression.



## Digital Security

**A**s internet use rises amid the COVID-19 pandemic, concerns on the safety of citizens on the internet also rises since more intensive use exposes users to higher potential of threats or attacks through digital media or in the digital space.

In 2020, SAFEnet began documenting incidents of digital attacks in Indonesia. We do this by opening up reporting channels through online forms, direct messages on Twitter and Instagram, as well as through a hotline phone number. We also monitor news updates through social media and online news sites. In cases involving high-risk individuals, such as activists, journalists, civil society organizations, indigenous people, or other critical voices, we will conduct multiple verifications, especially if a threat or attack is closely tied to their stance on an ongoing situation.

Working closely with a number of individuals and institutions

concerned with digital security impact on civil society, SAFEnet also operates a Quick Reaction Team (Trace) to respond to these reports. In some incidents, Trace was immediately successful, but in other cases it required a more complex and rigorous effort to respond.

### Findings

Our monitoring throughout the year reaffirms our previous findings of the digital space being an important tool for civil society to drive change. However, it has also become a medium of repression against civil society, including through cases of digital attacks.

Digital attacks can be classified into two categories: a hard attack and a soft attack. A hard attack involves specific skills and equipment to attack a target or even take over their asset. This includes cracking and hacking, tapping, and DDoS (distributed denial-of-service) attacks. Not everyone can carry out hard attacks as it requires specific skills and technology. A successful hard attack is usually one that is done without the victims ever finding out they have been targeted.

A soft attack, on the other hand, is employed to intimidate a target psychologically or publicly damage their

credibility. As such, this type of attack must be carried out openly using social media, sometimes anonymously. Examples of soft attacks include doxing, impersonation, and trolling by online mobs. A soft attack is usually coordinated and employs bots and anonymous accounts.

### Momentums

Throughout 2020, SAFEnet recorded at least 147 digital attacks—an average of 12 incidents a month. October saw the highest number of incidents occurring with 41 while only three occurred in March. On a month-to-month basis, the number of cases does not suggest any immediate patterns. However, it does indicate an upward trend and is closely affected by political situations and dynamics and can be grouped into three different momentums.

The first one was public reaction toward the Jobs Creation Omnibus Law, which sparked resistance among civil society and led to a wave of demonstrations and criticisms online on social media platforms. Online disapproval of the bill was aggregated through the use of hashtags such as #TolakOmnibusLaw (“Reject the Omnibus Law”) and #MosiTidakPercaya (“Motion of No Confidence”) which became trending topics on Twitter.



## Digital attacks throughout 2020

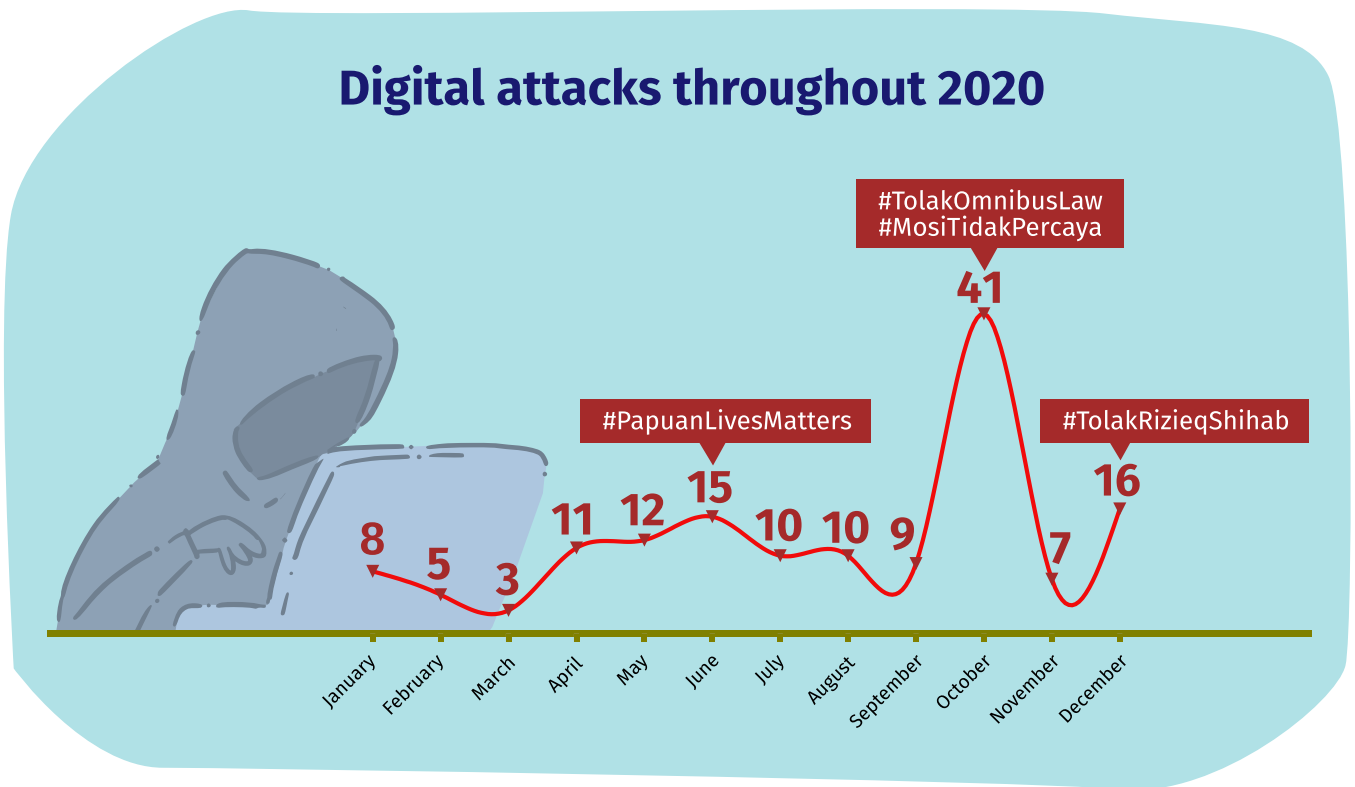


Figure 8: Number of digital attack throughout 2020.

The massive resistance was unfortunately met by rampant digital attacks targeting students, activists, and civil society organizations. Reports of WhatsApp account hacking was particularly common, such as in the case of Fajar Adi Nugroho, who was Head of the Student Executive Board of Univer-

sitas Indonesia (BEM UI). We also recorded attacks on websites and social media accounts of civil society alliances, such as found in the cases of the Indonesian People's Faction ("Fraksi Rakyat Indonesia") and Clean Indonesia ("Bersihkan Indonesia").



*Public disapproval of the Jobs Creation Omnibus Law on social media contributed to rampant digital attacks in 2020*

The second momentum that triggered the rise of digital attacks in 2020 was the anti-racism against Papuans movement in June, during which SAFEnet recorded a total of 15 incidents. While the campaign had its peak in 2019, it regained the momentum following the killing of George Floyd by police in the United States, reinvigorating movements across the world under the #BlackLivesMatter banner. In Indonesia, this was adapted into empowering

its own #PapuanLivesMatter movement.

Civil society groups took various actions and held discussions, especially online, due to the ongoing COVID-19 pandemic. However, organizers of discussions on the Papuan issue often received threats both verbally and digitally. Some of these attacks include the cases of student press activists of Teknokra Universitas Lampung and ac-

tivists of the Association of Journalists for Diversity (Sejuk), who had their social media accounts on Instagram, Facebook, WhatsApp, and even the ride hailing application GoJek attacked by unknown parties.

The third momentum was related to the COVID-19 pandemic. Throughout the year, many digital attacks were recorded targeting citizens and media organizations who published criticisms of the government handling of the pandemic. This peaked in August with three online media companies—Tempo.co, Tirto.id, and Kompas.com—targeted in a series of digital attacks following the publication of articles that are critical of a COVID-19 drug discovery claim made by Universitas Airlangga, the National Intelligence Agency (BIN), and the Indonesian Armed Forces (TNI).

Tempo.co was hit by a defacing attack and Tirto.id had two articles previously published abruptly removed from its website by the attackers. Not long after, epidemiologist Pandu Riono who was known for his criticisms toward the government handling of COVID-19 found social media account hacked overnight. Upon publishing an independent report of the government pandemic response, website of the re-

search group Center for Indonesia's Strategic Development Initiative (CISDI) was also targeted in a digital attack.

In comparison, data published by the National Police through their Cyber Crime Directorate also recorded incidents of digital attacks, which included reports of illegal access (138), theft of personal data (39), illegal interception (24), hacking of electronic systems (18), and defacing (9).<sup>37</sup>

In a broader sense, Tempo magazine reported up to 4,341,000 incidents of digital attacks occurred during the year, which is 51% higher than the number recorded in 2019.<sup>38</sup> Regionally, Kaspersky Security Network report found 111,682,011 local “trial” incidents on computers of Kaspersky users in Southeast Asia, with 20,264,000 targeting users in Indonesia. Globally, 32% of digital attacks were identified to be web-based and the remaining 68% via email.

In an ever broader sense, the National Cyber and Crypto Agency (BSSN) recorded a total of 316,167,753 digital attacks throughout the year, with 217,781 being attacks by malicious software or malware.<sup>39</sup> However, another data point from the Agency reported 475 million digital attacks in 2020, three times the

<sup>37</sup> <https://patrolisiber.id/home>.

<sup>38</sup> TEMPO Magazine.

<sup>39</sup> National Cyber and Crypto Agency (2020) *Laporan Tahunan Honeynet Project*.

number recorded in the previous year, with 2,549 cases of phishing, 79,439 compromised online accounts, and 9,749 defaced websites.<sup>40</sup>

Onward, this report will analyze the data collected through SAFEnet independent monitoring in 2020 with an emphasis on the political aspect of digital attacks over technicalities.

### Types of Attacks

Digital attacks that were recorded in 2020 were mostly hacking incidents, found in 114 cases (77.55%), followed by doxing with 14 incidents (9.52%),

DDoS attacks (2.72%), theft of personal data (2.72%), impersonation (2.04%), and others.

While hacking is a common terminology often used to refer to any types of digital attacks, in this context it is defined as any attempts to penetrate or take control of the digital assets of a target. In several incidents, such as in the cases of Tirto.id articles removal and Tempo.co defaced website, the hackers successfully penetrated their target's digital asset. In others, a hacking could be done as an experiment on a target.

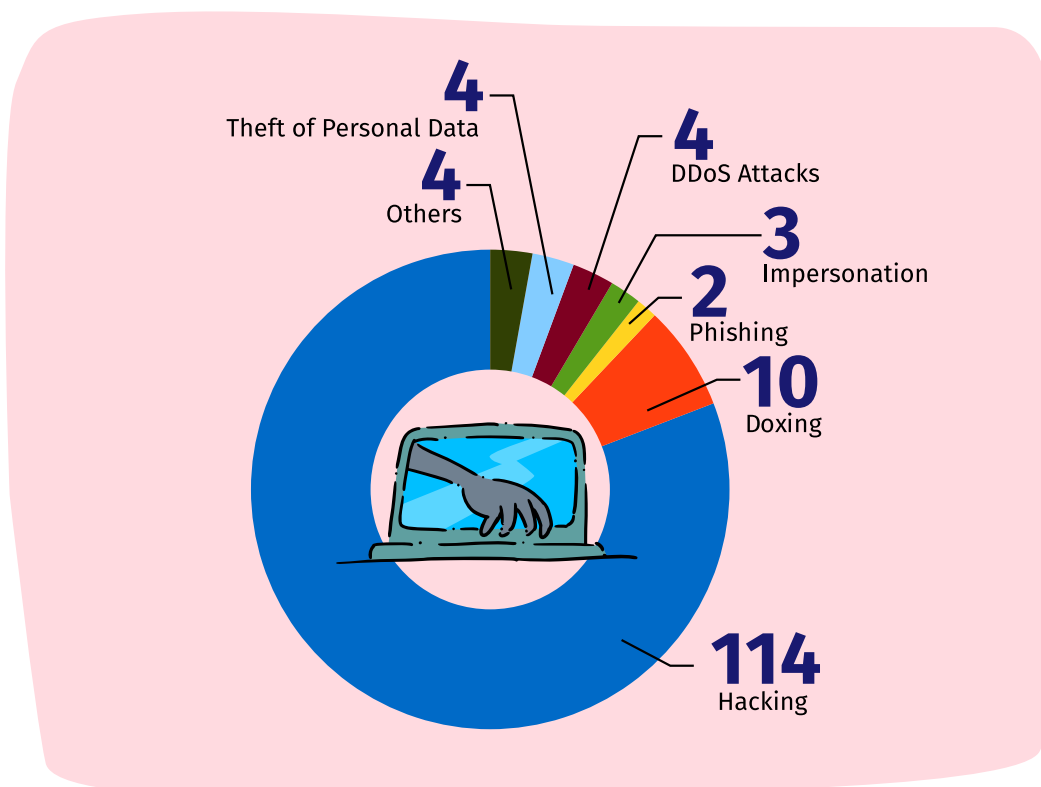


Figure 9. Types of digital attacks recorded in 2020.

<sup>40</sup> Harian Kompas, Monday, 22 March 2021.



In many incidents, hacking was used to take over the control of a target's digital asset, most commonly WhatsApp, Twitter, and Instagram. When this happens, the target will lose access and control of their digital account, such as seen in the case of Rasio Patra in April 2020. At the time, Rasio lost access to his WhatsApp account, which was then used to send out a broadcast message containing incitement to violent riot. Rasio was later arrested and detained by the police for 33 hours before being released following pressure from civil society.

SAFEnet also recorded some unsuccessful attempts of hacking, which occurred to the Instagram and Telegram

accounts of the civil society organization Indonesia Corruption Watch (ICW) in July 2020 and the Instagram account of Bali Legal Aid Institute (LBH Bali) in October 2020. Quick mitigation strategy from both parties was proven effective in preventing the hacker from taking over control of their digital assets.

### Targeted Platforms

In terms of platforms, websites were the most targeted with 45 incidents (30.61%), followed by WhatsApp with 33 incidents (22.45%), Instagram with 24 incidents (16.33%), Twitter with 19 incidents (12.93%), other platforms with 17 incidents (11.56%), and Facebook with 14 incidents (9.52%).



Picture: Anton Muhajir

*After websites, text messaging application WhatsApp was the second most targeted platform in cases of digital attacks.*



Other platforms that have also been targeted include GoJek accounts, cell phones, and online game accounts. There were also other cases in which SAFEnet was unable to identify the targeted platform as the victims did not specify the platform they were targeted on.

Ironically, the high number of attacks on websites was identified as mostly government websites. Attacks on government websites particularly peaked as public disapproval over the passing of the Jobs Creation Omnibus Law was intensifying, with at least 12 government websites, including that of the

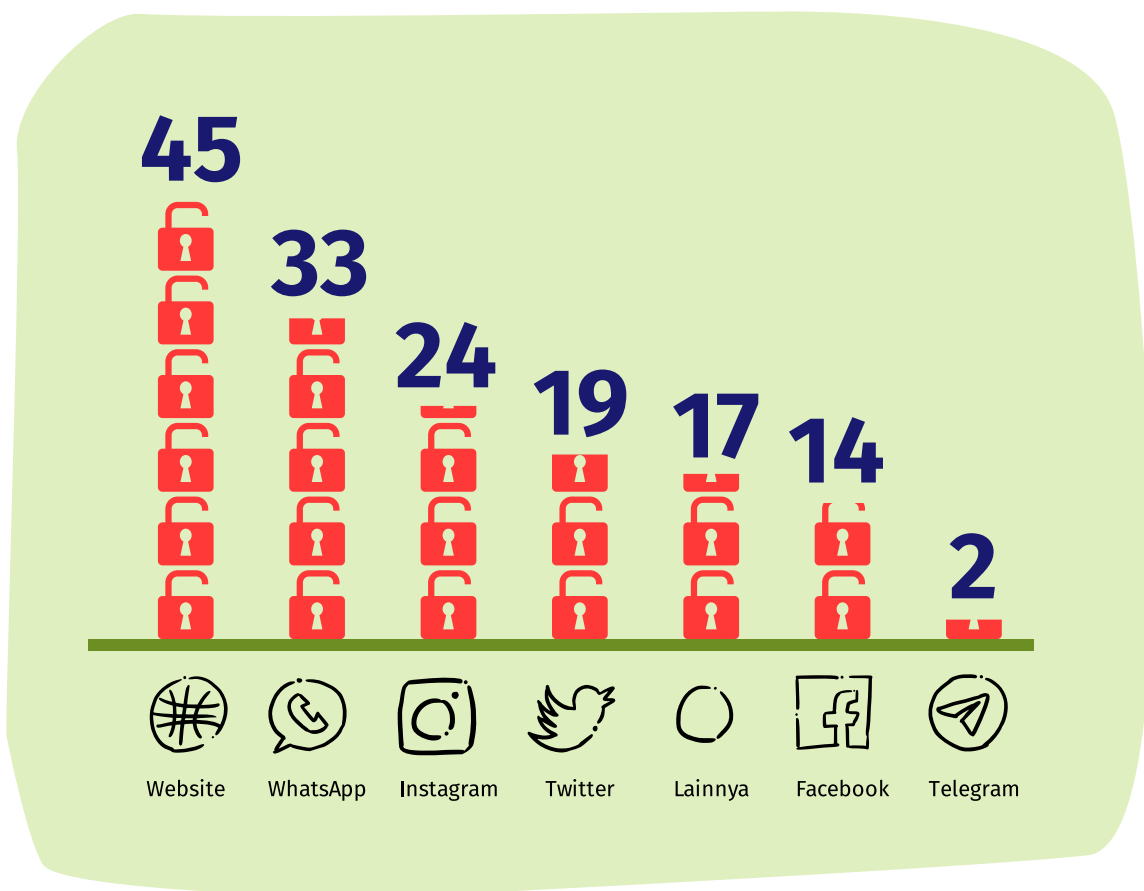


Figure 10. Targeted platforms of digital attacks in 2020

Parliament, the Ministry of Health, and several local government offices, were defaced by hackers who instead display text to reject the Jobs Creation Omnibus Law.

Another mass attack also took place in December, with 10 government websites defaced by a hacker who claimed to be part of a group called the Rasullullah Council and the NU Cyber Army, displaying text to reject the return of controversial cleric Rizieq Shihab to Indonesia.<sup>41</sup> These cases are consistent with our previous finding that digital attacks in Indonesia are increasingly political in nature.

Meanwhile, platforms such as WhatsApp and Instagram are often targeted possibly due to their popularity with users, with WhatsApp being the most popular text messaging application in Indonesia with around 143 million users,<sup>42</sup> including students, activists, and journalists. The many hacking incidents targeting WhatsApp accounts of student activists in October could be explained by their involvement in the demonstrations against the Jobs Creation Omnibus Law earlier in the month.

In some cases, digital platforms could also be used as a medium to facilitate an attack, especially in more subtle at-

tacks that include impersonation on Facebook, doxing on Twitter, and making threats on Instagram.

In other cases, an attack could also be carried out targeting multiple platforms, such as in the case of a Tempo magazine journalist who experienced disturbances on their social media accounts, email, and also text messaging applications in December 2020. The attack came after the journalist published a report uncovering government corruption of the COVID-19 social assistance fund.

### Background of Victims

Based on SAFEnet monitoring data in 2020, the victims of digital attacks are grouped by their backgrounds into categories such as government, regular citizen, activists, journalists, students, civil society organizations, and others. This is necessary to help us with our analysis and identify the most vulnerable groups to digital attacks. In doing so, we recognize that some individuals may qualify to be grouped into more than one background category, such as a student-activist, a journalist-activist, and a student-journalist.

Overall, we found that government institutions are targeted the most with 38 incidents (25.85%), followed by regular citizens with 30 incidents

41 <https://cyberthreat.id/read/9618/10-Website-Pemerintah-Daerah-Diretas-Hacker-Anti-Rizieq-Shihab-dan-FPI>

42 <https://www.merdeka.com/teknologi/pengguna-Internet-indonesia-83-%nya-pakai-whatsapp.html>

(20.41%), journalists with 26 incidents (17.01%), activists with 25 incidents (17.01%). %), university students with 19 incidents (12.93%), and civil society organizations with 15 incidents (10.20%). Note that in our analysis, groups such as public foundations, civil alliance, and civil movement are grouped as civil society organizations.

While government agencies are the most targeted, in a broader perspective, the data indicate that those who are perceived as critical voices—journalists, activists and university students, as well as civil society organizations—remain the most vulnerable to digital attacks with a combined total of 66 incidents (44.90%). This

was particularly true in 2020 as critical voices were very active in scrutinizing government handling of the pandemic, expressing solidarity with Papuan causes, and denouncing the Jobs Creation Omnibus Law.

What this indicates further is that digital attacks in 2020 did not just happen to target anyone. The attacks actively target individuals who are critical of government policies, suggesting that digital attacks continue to be used to repress critical voices in the society. Unfortunately, it is difficult to analyze the data further given that most, if not all, of these digital attacks are asymmetrical in nature with the perpetrators not identified by law enforcement.



Figure 11. Victims of digital attacks in 2020 by professional backgrounds

## Health vs Privacy

In addition to digital attacks, another digital security that came to prominence during the COVID-19 pandemic was privacy violations experienced by some citizens in the facade of handling the pandemic. An issue that has been a point of contention globally, not only in Indonesia, it presents a dilemma for governments who are responsible for public health but also at the same time cannot violate its citizens' right to privacy.

On 30 March 2020, the Indonesian government launched the PeduliLindungi application to track COVID-19 exposure, which was developed by the state-owned PT Telekomunikasi Indonesia for smartphone users.

Utilizing Bluetooth feature on smartphones, PeduliLindungi works by detecting other people nearby a user. Users are notified by the app if they have been to a location or encountered anyone who have tested positive or are under surveillance for possible COVID-19 infection. It can also detect if the user is in a COVID-19 hotspot or whether the user has completed self-quarantine or isolation period.

While potentially useful in curbing the spread of COVID-19, the application has attracted attention for its lack of

clarity in terms of user privacy protection and security. In the wake of this issue, SAFEnet along with 12 other civil society organizations sent out an open letter to the Ministry of Communications and Informatics 26 June 2020.<sup>43</sup> The government responded to our collective demands by introducing a privacy policy to the application.<sup>44</sup>

In terms of security, an analysis by the Citizen Lab, an interdisciplinary laboratory at the University of Toronto, Canada, found that the user permissions requested by the application are deemed “dangerous”, with some providing no clarity as to why certain access is necessary at all.<sup>45</sup>

The Citizen Lab highlighted three user permissions that the application request from its users: (1) location access that can record geolocation, (2) camera access to take photos and record vide-

os, and (3) device storage access to read to read photos and files. While access to location and camera are understandable in order to be able to track locations and scan QR codes respectively, user permission request to “read\_external\_storage” and “write\_external\_storage” are not necessary at all.

It should be underlined, however, that The Citizen Lab’s analysis was published on 21 December 2020 based on the Android version 2.2.2 of the application. The Ministry of Communications and Informatics has since claimed that the application has now been updated to version 3.1.1 with improvements in features and user permission.<sup>46</sup> As of early 2021, the application has been downloaded by more than 1 million users on Google Play Store.

---

43 <https://www.article19.org/resources/indonesia-open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/>

44 <https://pedulilindungi.id/kebijakan-privasi-data>

45 <https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/>

46 <https://tekno.kompas.com/read/2021/01/07/09090047/diperbarui-aplikasi-pedulilindungi-tak-akses-bluetooth-hingga-kamera-lagi?page=all>



## Drastic Increase in Online Gender-Based Violence during the Pandemic

**S**AFEnet monitoring data found that online gender-based violence has worsened during the pandemic, rising by over ten-fold from 60 incidents in 2019 to 620 incidents in 2020.

Data published by the National Commission on Violence against Women suggest the same grim conclusion. In its 2020 annual report, the Commission received 940 reports of online gender-based violence incidents, almost four times the 241 incidents recorded in the previous year. Both data sets from SAFEnet and the National Commission suggest an average of two to three incidents per day in 2020.



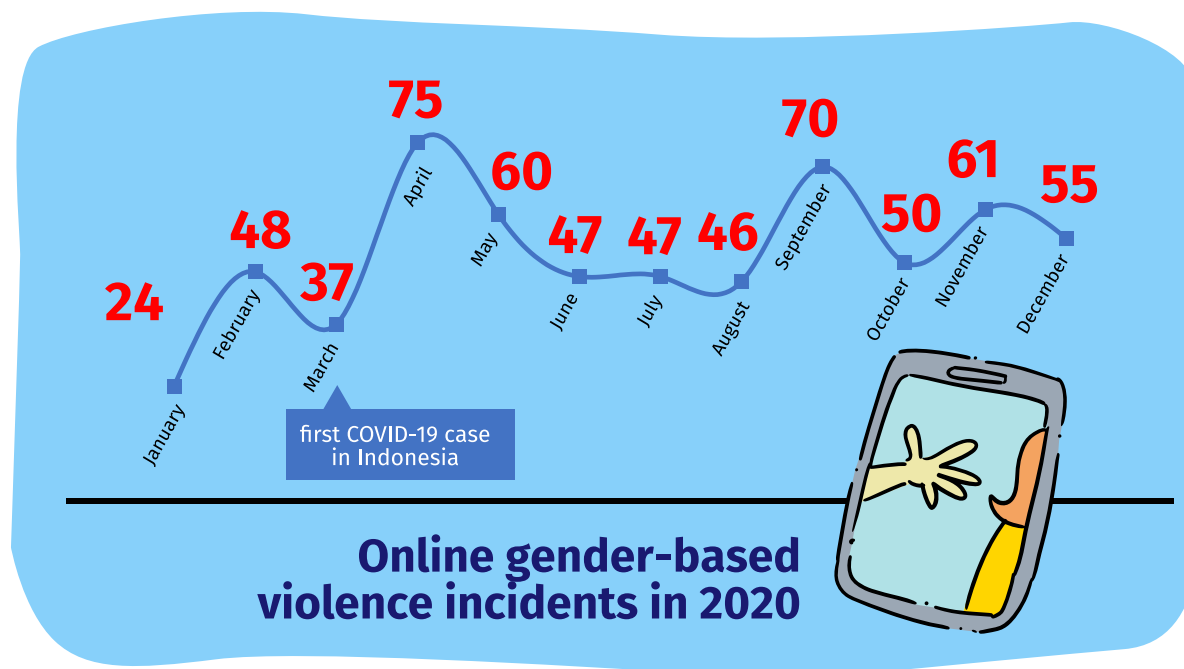


Figure 12. Online gender-based violence incidents in 2020

Of the 620 cases that were recorded by SAFEnet, 248 were referrals from the National Commission while 372 came in directly via SAFEnet's reporting channels—Instagram, WhatsApp, Telegram, email, and online forms. In addition to higher public awareness of online gender-based violence, the drastic increase could also be explained by SAFEnet's more intensive monitoring through the various available channels throughout the year.

Overall, non-consensual dissemination of intimate images (NCII) was the most prevalent and dominant form of online gender-based violence, identified in 468 cases or more than 75% of all the cases, recorded by SAFEnet.

Deeper analysis indicates that NCII is motivated by various factors. In 208 cases, there are no specific motives that could be identified as the perpe-

trators are unknown. In 149 cases, the motive was identified as threats to prevent the victim from ending a relationship or to force the victim to rekindle a past relationship. In 119 other cases, the motive was identified as "sextortion", threatening to release private, intimate images in exchange for money, sexual favors, or more intimate images.

Furthermore, in 51 cases, SAFEnet documented another form of online gender-based violence which is intended to damage the victim's reputation. In this instance, the perpetrator would create fake online accounts with the victim's likeness attached to it and begin uploading inappropriate content impersonating the victim using photo manipulation to frame them with sexual narratives. SAFEnet also found cases of harassment by body shaming, bullying, and unsolicited sexual con-

tent in 46 cases, followed by instances of hacking, sharing personal data, and stalking with sexual motives in 38 cases.

Other forms of online gender-based violence that SAFEnet recorded in less than 10 cases included threats, scams with requests for intimate images, and so on.

For example, non-consensual dissemination of intimate images are often carried out with the intention of damaging the victim's reputation by impersonating and posting manipulated intimate content of them on social media.

In some other cases, we also found scam attempts in which the perpetra-

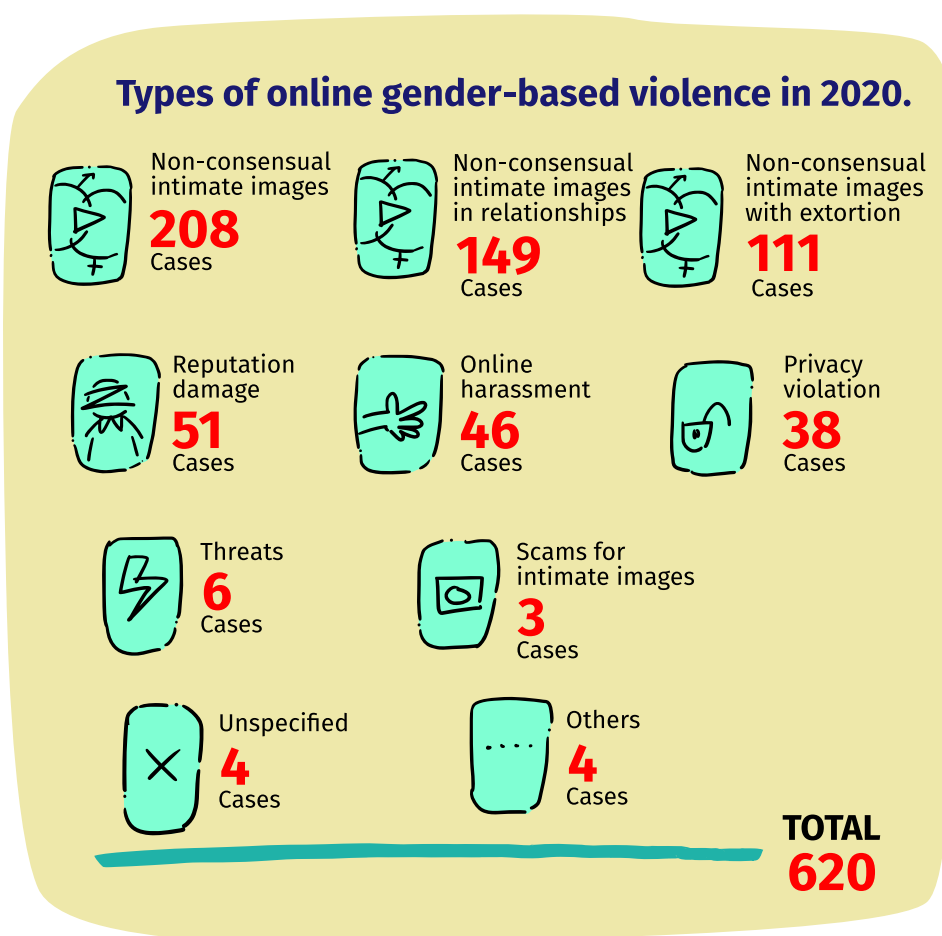


Figure 13. Types of online gender-based violence in 2020.

SAFEnet's data indicate that online gender-based violence rarely take only one form. In many cases, online gender-based violence manifests in a combination of several different types.

tor offers monetary compensation for the victim to send out their intimate photos without actually making any payment. Instead, the perpetrator would then use the intimate photos

they received to extort the victim into sending more intimate photos. The perpetrator would continue doing this with riskier demands the longer the victim is under their control.

Overall, victims of online gender-based violence identify as women (472 victims or 76.13%) and men (31 victims or 5%). In the remainder of all the other cases SAFEnet recorded, the victims chose not to specify their gender.

The disproportionately high number of victims who identify as women further proves that women are more vulnerable to becoming victims of online gender-based violence, while men make up a dominant portion of the perpetrators, from strangers, ex-spouses, husbands, to boyfriends. SAFEnet also recorded some cases in which the perpetrators and victims were gay men and lesbian women who do not want

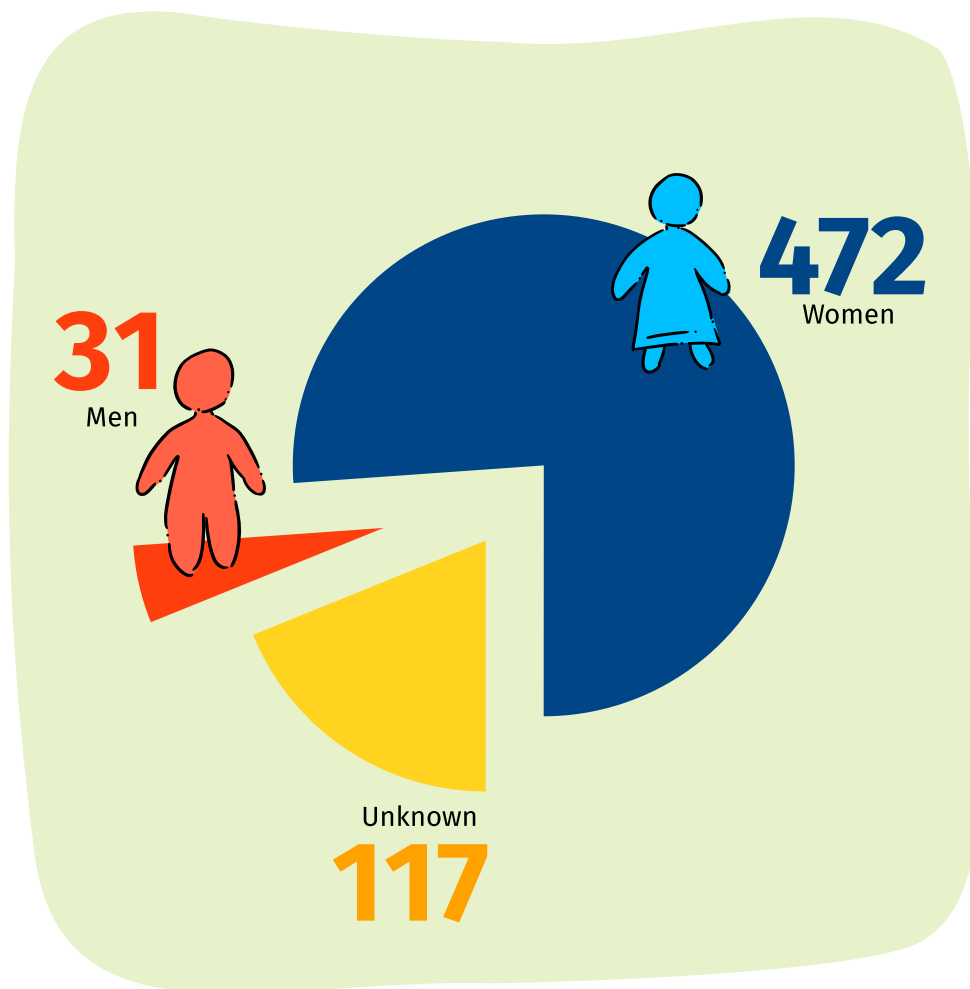


Figure 14. Background of victim of online gender-based violence in 2020.





their ex-partners to date the opposite sex.

In terms of age, nearly half of the reports (47.1%) did not specify the age of the victim. As for those who list their age, most are in the 21–30 age group with a total of 192 people (30.97%), followed by 14–20 with 119 people (19.19%), 31–40 with 11 people (1.77%), and 41–50 with 6 people (0.97%). This breakdown suggests that most of the victims are people who are still in their productive age.

It is important as well to note the number of children identified as victims of online gender-based violence, with 54 (8.71%) identified as below 18 years of age. Of these, the youngest were two junior high school students who were born in 2006, both falling victims to strangers and friends whom they knew through online games, text messaging applications, and social media.

The use of online games as a tool of finding underage victims in online gender-based violence cases is relatively small, especially compared to social media, text messaging applications, and dating sites. Nevertheless, it is important to be cautious of how it could be abused by perpetrators of online gender-based violence.

In the wake of the drastic increase in the number of non-consensual disse-

mination of intimate images case reports, SAFEnet released a guide for victims on [awaskbgo.id/ncii](http://awaskbgo.id/ncii) link in October 2020.

### **Restricted Access**

Throughout 2020, SAFEnet also monitored cases of online gender-based violence among minority groups, particularly the Lesbian, Gay, Bisexual, Transgender, and Queer (LGBTQ) community. Unfortunately, our observation indicates that the internet is still not a safe space for LGBTQ individuals. We found many LGBTQ-oriented websites and social media accounts being forcibly removed or taken down by platforms for indecency or hate speech.

On social media, the use of hashtags that are associated with support for LGBTQ people such as #YouAreNotAlone, #LoveWins, and #StickerRainbow have instead led to hatred against LGBTQ people and reported to the platform.

We also found cases of access restrictions based on gender identity. The SBF group in Karawang, West Java, for example, was removed by Facebook for indecency because of their lesbian community content. The group's account owner was also summoned by local police in June 2020. In the same month, F, who lives in Serpong, Banten, was also summoned by local police for circulating an invitation to a gay party on Facebook. Previously in April, BA, who lives in Probolinggo, East Java,



was summoned by local police for posting their experience being threatened by the police.

Ironically, while expressions by gender minority groups are being policed, threats directed at LGBTQ people on these platforms are not. There are even groups that deliberately monitor and report individuals who they deem as propagating LGBTQ values, such as the Manguni 123 Lovers group, which has more than 60 thousand members who do not only interact online but also offline. This group reported at least three people in 2020 to the authorities, further threatening the rights of minority groups from freely expressing their gender identity in the digital space.

### **Media Persecution**

SAFEnet also recorded several news reports throughout the year that have continued to perpetuate the climate of persecution against gender minorities through insensitive narratives that often adds to the violence experienced by victims of online gender-based violence.

The most common forms of violence in this context have been violations of privacy and gender identity. A well-known incident involves the celebrity LL whose public persona is consistently linked to questions surrounding their gender identity. Law enforcement, in cases involving gender mino-

rities, also commit these forms of violence as they deliberately conceal anyone's gender identity, well knowing that it could pose them to risks and threats.

Such privacy violations were also committed by news media in their reports regarding FP, a social media persona who pranked members of certain gender minority group in Bandung, West Java. In their reports of the incident, many news outlets published reports that highlight the gender identity of the victims instead of the incident itself.

Similarly, many media reports of the circulation of intimate content involving public figures GA and MYD were also insensitive as they disclose the full names of both parties and even display their pictures despite both being victims of online gender-based violence in the form of non-consensual dissemination of intimate images

Reporting of this nature does not only violate their privacy rights, but also signals the failure of the media to empathize with the victims. In the status quo, while the media continues to perpetuate systemic violence against victims of gender-based violence through insensitive reporting, the Press Council has not taken any firm actions on gender insensitive reports that could very well be categorized as instances of gender-based violence itself.



## EPILOGUE

### Surviving Adversity

**T**he Economist Intelligence Unit ranked Indonesia's democracy at 64th among all the countries rated with a score of 6.3 out of 10. This marked the lowest rank for Indonesia since 2008 and placed the country in the "flawed democracy" category. Analysis from a number of well-known thought leaders could be used to explain the regression of Indonesia's democracy, showing gradual strangulation by populist leaders.

Some indicators that have been analyzed include the eradication of opposition parties through hegemony or force by Mietzner (2016), Power (2018), Mietzner (2019), and Aminudin (2020); the use of non-legal/liberal/criminalization methods to suppress populist Islamic groups by Mietzner (2018), Power (2018), Aspinall & Mietzner (2019), Warburton & Aspinall (2019), David MacRae et. al. (2019), and Aspi-

nall, Fossati, et al. (2020); the tendency to focus on infrastructure development and ignore human rights and environmental damages by Warburton (2016); the growth of anti-democratic ideology/groups by Hadiz (2017), Aspinall & Warburton (2018), Bouchier (2019), and Mietzner (2019); and the piracy of state institutions for the purpose of power by Power (2018) and Mietzner (2019).

The COVID-19 pandemic also put more pressure on the performance of Indonesia's democracy in 2020. Survey results of Indonesian Political Indicators on 7 June 2020 shows that during the pandemic, public satisfaction of Indonesia's democracy has plummeted compared to previous findings. Economic conditions and government handling of the COVID-19 outbreak could be considered as key factors to low public satisfaction of democracy, particularly in the early days of the pandemic. It further shows that the majority of the public agree (47.7%) and strongly agree (21.9%) that citizens are increasingly fearful of expressing their opinions.

Analysis and survey results indicating that Indonesia is moving away from democracy amid the pandemic are further reinforced by findings in this Indonesia Digital Rights Situation Report 2020. As explored throughout this report, the Indonesian government has continued to allow the digital rights of its citizens to be ignored or even violated. This clearly worsens the situation

for people in Indonesia, where lives are becoming increasingly difficult while the government moves very slowly.

The government's decision to implement distance learning for school children was not equipped with any provision for equal and adequate internet access for all. The digital divide continues to widen and makes it increasingly difficult for those who have been marginalized by their lack of access to information. On one hand, education is key to getting out of the poverty cycle, but digital divide impacts those who live in poverty the most. As a result, the problem continues to worsen, the privilege gap continues to widen, and the poor stays poor.

As if that was not enough, the government's policies on internet increasingly becoming authoritarian as well. Criticisms toward government policies are constantly met by counter-narrative campaigns. Digital sector regulations, such as the Communications and Informatics Ministerial Regulation No. 5 of 2020, are being exploited to allow the government unfettered access to censor and do as it sees fit with information circulating online, explicitly violating basic civil rights that are protected by international standards of human rights.

As citizens are forced to stay home during the pandemic, they are expected to continue working, studying, and

going forward with their lives digitally, but the government is leaving them exposed and vulnerable to a variety of threats, including digital attacks, which are often used to advance a political motive. Meanwhile, online gender-based violence has increased sharply.

As an organization that fights for the fulfillment of digital rights in the Southeast Asia region, including Indonesia, SAFEnet sees the recent development in Indonesia as signs of not only a return to authoritarianism, but more as a leap into the abyss of a democratic crisis.

Using the same disaster management system that the government uses in Indonesia, SAFEnet declares that Indonesia in 2020 has reached the second state of alert in facing digital authoritarianism. It is therefore necessary for us to reiterate this so that the democratic setback can be undone.

We also condemn the continuous neglect of the government toward the rampant digital authoritarianism practices. This includes the introduction of new policies and regulations that have

led to the shrinking of civic space, where repressive laws have claimed countless victims over time.

Civil society groups must strengthen themselves and install the necessary skills to be able to survive. Cyber resilience in the form of capacity building initiatives for activists to master the foundations of digital security is an important agenda that must be prioritized collectively.

Initiatives through reviews and appeals of laws that affect us as well as continued advocacy for better cyber regulations must continue to protect public interests and to fight back against unlawful restrictions that the government has imposed on its own citizens' constitutional rights in the digital space.

All in all, civil society groups also needs to strengthen collaborations with other human rights defenders in regionally and globally to curb the impact of weakening democracy around the world. A global solidarity is the antivirus to authoritarianism.











**SAFE**net

SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK