DIGITAL RIGHTS IN INDONESIA: 2023 SITUATION REPORT

THE ELECTION COLLATERAL DAMAGE

SAFEnet

DIGITAL RIGHTS IN INDONESIA: 2023 SITUATION REPORT

THE ELECTION COLLATERAL DAMAGE

Digital Rights in Indonesia: 2023 Situation Report
THE ELECTION COLLATERAL DAMAGE

Februari 2024

REPORT WRITING TEAM
Coordinator & Editor:
Anton Muhajir

Writers:
Andreas Takimai
Nabillah Saputri
Nenden Sekar Arum
Shinta Ressmy
Tessa Ardhia M
Unggul Sagena
Widayanti Arioka

Illustration:
Bram Kusuma

Design and Layout:
Crueniaone

Translation:
Kate Walton

Publisher
Southeast Asia Freedom of Expression Network (SAFEnet)
Jalan Gita Sura III Nomor 55 Peguyangan Kaja
Denpasar, Bali 80115

+62 811 9223375
info@safenet.or.id
𝕏 & @safenetvoice
safenet.or.id

TABLE OF CONTENTS

Foreword

General elections in the modern era cannot be separated from the use of information and communication technology (ICT). This is the case for the 2024 General Election in Indonesia. Digital technology is useful for everyone involved in this 'festival of democracy', occurring every five years. For citizens as voters and constituents, this technology helps them find information about elections themselves, including the stages, mechanism, and, of course, legislative candidates as well as the candidate pairs running for president and vice president.

For those responsible for running elections – including the General Election Commission (*Koalisi Pemilihan Umum*/KPU), the General Election Supervisory Agency (*Badan Pengawas Pemilu*/*Bawaslu*), and the Honorary Council of Election Management Bodies (*Dewan Kehormatan Penyelenggara Pemilu*/DKPP), digital technology assists with planning, implementation, vote counting, and oversight. Finally, for electoral candidates, including legislative, presidential, and vice presidential candidates, digital technology functions to introduce themselves and their visions to voters.

Seeing the important role played by digital technology in the 2024 General Election, it is therefore critical that human rights in the digital sphere are respected, fulfilled, and protected by the state. SAFEnet refers to 'digital rights' as covering three main rights: the right to access the internet, the right to freedom of expression, and the right to feel safe.

As a result, whether we like it or not, the 2024 General Election is impacting our digital rights. This *Digital Rights in Indonesia: 2023 Situation Report* centres our attention on the election by asking one key question: how did the 2024 General Election impact our digital rights in 2023?

This question emerged because around one year ago, indications appeared that the 2024 General Election would have an impact on digital rights. The establishment of the Cyber Troops 08 group (*Pasukan Siber 08*) by supporters of presidential candidate Prabowo Subianto is just one example. These 'troops' did not just act as a search engine for information on Prabowo, but also 'hunted down' those who were considered to be smearing Prabowo's good name or undertaking negative campaigns against him in the digital sphere. The 08 Troops worked to find the 'perpetrators', including their names and IP addresses, something which should only be carried out by law enforcement agencies.

Online gender-based violence has also been occurring. One female legislative candidate in East Nusa Tenggara (NTT) withdrew her candidacy after her personal video was disseminated on social media. This case is probably just the tip of the iceberg, with other cases in other areas hidden from sight.

Using SAFEnet's framework, this report on the digital rights situation is divided into four categories: internet access, freedom of expression, digital security, and online gender-based violence.

To find answers to our question, SAFEnet used the method we have used for the past five years to monitor the digital rights situation in Indonesia. First, we use the aduan.safenet.or.id complaints platform, which was established in 2021. Through this platform, citizens can report digital rights violations which they themselves or someone else experienced. Second, through social media and mainstream media, we document and investigate reports to ensure accuracy of data and facts.

Third, SAFEnet also performs direct monitoring and assistance in the field. In line with our organisational mandate, SAFEnet provides case management and support for victims of digital rights violations. Not only do we record cases, SAFEnet also provides direct assistance to victims of online gender-based violence, digital attacks, or criminalisation as a result of their digital self-expression.

The results of our monitoring are published in two forms: quarterly reports and annual reports. The quarterly reports consist of case data and analysis for the previous three months. The aim of these reports is to provide the public with quick access to information on the digital rights situation, especially if there is an important case or event. The annual situation report, meanwhile, does not only compile all of our monitoring from the calendar year, but also explores the context so that the public can obtain more detailed information on the digital rights situation of the past year.

Through these reports, we hope that the public becomes more aware of the importance of digital rights as one component of human rights. More specifically, we hope that issues of digital rights become more important in the public and policy agendas, including in the 2024 General Election.

Denpasar, February 2024

About SAFEnet

Southeast Asia Freedom of Expression Network (SAFEnet) is a civil society organisation which defends for digital rights, including the right to access the internet, the right to freedom of expression, and the right to feel safe in digital spaces. SAFEnet is a legally-registered association with the name *Perkumpulan Pembela Kebebasan Asia Tenggara* and is located in Denpasar, Bali.

SAFEnet's vision is the realisation of a digital space that upholds human rights values for all. To achieve this vision, SAFEnet implements four main programs: policy advocacy to support the fulfilment of digital rights; support for victims of digital rights violations; capacity building for civil society on digital rights; and solidarity for civil society who are fighting for human rights.

SAFEnet has consistently advocated for victims of digital rights violations and been active in advocating for internet policies to include human rights perspectives. Since 2019, SAFEnet has also provided holistic security training (physical, psychosocial, and digital) for vulnerable groups in Indonesia and Southeast Asia to build their resilience towards increasingly common digital repression.

As of February 2024, SAFEnet has 34 members and 15 volunteers from a wide range of backgrounds, including journalists, bloggers, university lecturers, environmental activists, students, IT practitioners, transgender activists, and others. They are located in 20 cities across the Indonesian archipelago, reaching from Medan to Jayapura.

Currently, SAFEnet has four divisions: the Internet Access Division, the Freedom of Expression Division, the Digital Security Division, and the Equality and Inclusion Division. These four divisions work to monitor digital rights violations, provide training on digital security, assist victims of digital criminalisation and online gender-based violence, and build networks at the national, regional, and international levels.

Nationally, SAFEnet is involved in the Journalist Safety Coalition (*Koalisi Keselamatan Jurnalis*), the Coalition for the Serious Revision of the Electronic Transactions and Information Law (*Koalisi Serius Revisi UU ITE*), the Coalition of Advocacy for Personal Data Protection (*Koalisi Advokasi Perlindungan Data Pribadi*), the Quick Response Team (*Tim Rekasi Cepat*/ TRACE), and others. SAFEnet is also a member of the Asia Democracy Network, the Keep It On Coalition, the Stop Digital Dictatorship Coalition, and several regional and international forums.

Summary

The Election Collateral Damage. The title we have given the *Digital Rights in Indonesia: 2023 Situation Report* clearly illustrates the condition of digital rights in Indonesia over the past year. SAFEnet's monitoring throughout 2023 found that the 2024 General Election has served to worsen violations of digital rights in Indonesia across four categories: internet access, freedom of expression, digital security, and online gender-based violence.

First, the topic of internet access. The 2024 General Election has made strong use of information and communication technology (ICT) to support its implementation. Online information about the election became key, in line with the growth in the number of people using the internet. However, the increase in users and use of the internet, including in the context of the 2024 General Election, unfortunately has not been balanced by equal availability and accessibility. For example, some residents of Gunung Kidul in the Special Region of Yogyakarta, do not have reliable internet access, even though the KPU of Yogyakarta will be using a digital vote counting system in 2024.

In 2023, internet access disruptions continue to occur. At least 63 incidences were recorded, including 49 infrastructure disruptions, seven service disruptions, and seven policy-based disruptions. Protected internet access disruptions were also compounded by a variety of 'force majeure' situations, both one-off and repeated.

Another problem is the continued reduction in internet speed in Indonesia. In November 2023, Indonesia fell in its internet speed ranking, to be ranked 100 out of 141 countries. The Minister for Communications and Information stated that Indonesia's average internet speed is just 22 Mbps, far below the global average of 100 Mbps.

In terms of internet services, the increase in the number of internet service providers (ISPs) has not been accompanied by improvements in customer service. ISPs remain limited in number in the more remote areas of Indonesia, as do the number and reach of mobile operators. The death of 3G services – which forced users to shift to 4G – was also not offset by an increase in 4G transmitter towers.

Second, freedom of expression. In 2023, the trend was an increase in the number of politically motivated complaints made to police in the leadup to the 2024 General Election. Complaints were dominated by party institutions/organisations and sympathisers using articles of defamation and hate speech. Complaints predominantly targeted politicians and netizens who used their social media accounts to express themselves or share their opinions on the political condition in Indonesia.

In 2023, criminalisation of digital expression increased compared to the previous year. The number of complaints in 2023 increased by 15.9 percent, with a total of 126 people reported to the police. This limited the right to freedom of expression and opinion, which is guaranteed by the International Covenant on Civil and Political Rights (ICCPR), the 1945 Indonesian Constitution, and Law no. 39/1999 on Human Rights (UU HAM).

Based on SAFEnet's observations, trends in digital criminalisation through to 2023 continued to increase with the usage of problematic articles in UU ITE. Almost half of the cases recorded in 2023 – or 41.22 percent, to be exact – used Article 27 clause 3 of UU ITE. Following this was Article 28 clause 2 of UU ITE, which was used in 24.56 percent of cases. Article 27 clause 1 of UU ITE, Articles 14-15 of Law no. 1/1946, and Article 45 clause 3 of UU ITE were also frequently used as the basis of complaints.

This practice of criminalisation is also marked by the imbalances in power relations between complainants and targets of complaints. Ordinary citizens were those most often reported to the police, followed by content creators and students. In terms of complainants, organisations/institutions made the most complaints, followed by public officials and business people/businesses.

Social media was the platform most commonly used as evidence in complaints made to police over the reporting period, with 64 complaints (56.14 percent) made referring to social media posts. Press releases, messages sent in chat applications, and other forms of evidence were also used. Frustratingly, there were also several victims of criminal acts who were reported to the police under UU ITE because of the complaints they had made.

Third, with regard to digital security, there was an increase in the number of digital attacks, both soft or psychologicall attacks and hard or technical attacks which targets the victim's digital assets. In the context of the 2024 General Election, several digital attacks specifically targeted the accounts of electoral candidates as well as accounts which discussed politics. For example, the accounts of a legislative candidate from the Workers' Party in Surabaya, East Java and Butet Kartaredjasa, an actor and comedian, who had previously been warned by police for discussing politics on her platform. There were also several state institutions which experienced data leaks, including the General Election Commission, the People's Representative Council, and the National Police.

SAFEnet found that digital incidents and attacks occurred 323 times in 2023. This is an increase on previous years, with 302 cases recorded in 2022, 193 cases in 2021, and 147 cases in 2020. In 2023, on average 27 digital attacks and incidents occurred every month.

The most common method of attack, especially in the months of July and August 2023, was a systemic attack, which used android package kit (APK) files. These were widely disseminated on WhatsApp groups, the members of which included ordinary citizens, citizens, and Papuan activists.

Digital attacks in 2023 primarily targeted public agencies, making up 21.67 percent of cases. This cannot be separated from data leak cases, with citizen data being sold on the dark web or hacker forums. Meanwhile, digital attacks targeting ordinary citizens made up 11.15 percent of cases.

Digital attacks on critical groups, including activists, journalists, the media, and civil society organisations (CSOs) also occurred in 2023. There were 23 cases (7.12 percent) which targeted activists or CSO staff; 12 cases (3.7 percent) which attacked journalists or media workers; and 15 cases (4.64 percent) which targeted the media. Attacks experienced by the media

included distributed denial of service (DDoS attacks) and the suspension of Twitter accounts.

Finally, online gender-based violence also impacted the 2024 General Election. MRRH, a female politician from East Nusa Tenggara (NTT) failed to continue her legislative candidacy after her intimate video was disseminated on several social media platforms, including Facebook, Twitter, and WhatsApp. After withdrawing as a candidate, she also resigned as a member of her party, Nasdem. Social media attacks on other female legislative candidates also occurred, exploiting the candidates' genders.

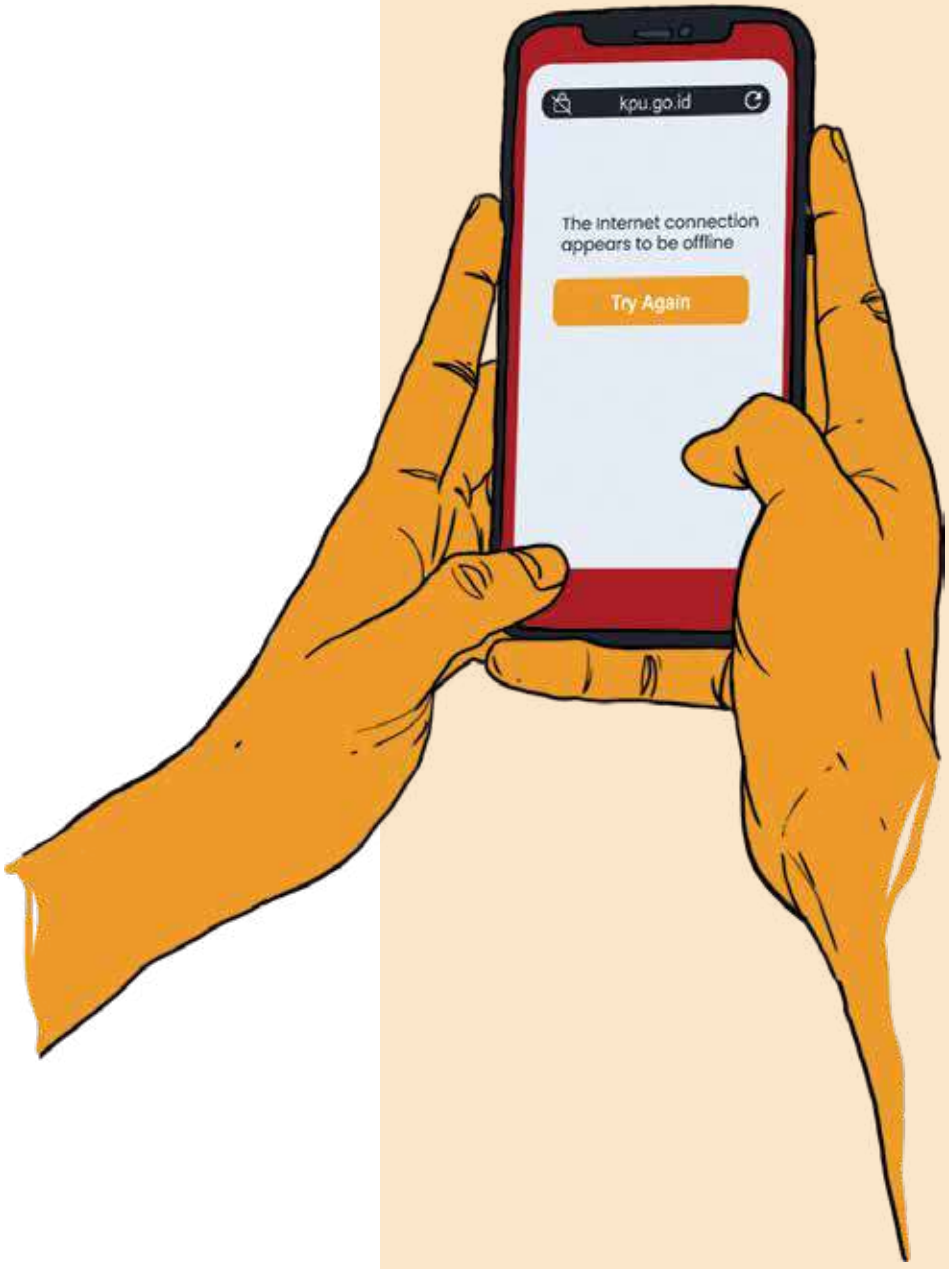
In terms of numbers, online gender-based violence (GBV) increased significantly. In 2023, SAFEnet received 1,052 complaints of online GBV. This represents a 33.65 percent increased on previous years, when 677 online GBV complaints were recorded in 2021 and 698 in 2022. The highest number of reports was received in July 2023, when 120 complaints were recorded.

Based on these 1,052 complaints received by SAFEnet, a total of 562 cases (53.42 percent) were experienced by victims aged between 18 and 25 years, while 230 cases (21.87 percent) were experienced by children aged 12 to 17 years. Meanwhile, the type of online GBV most commonly reported was image-based sexual abuse (commonly known as misuse of intimate content), representing 53.13 percent of cases. Extortion cases which threatened to share victims' sexual content ('sextortion') also widely occurred, making up 13 percent of cases.

The most commonly-used methods were extortion and intimate content manipulation through video-based sex calls. The manipulation of video calls was often structured and systematic, even targeting children as victims. It was not uncommon that online GBV was also perpetrated against vulnerable groups, including the dissemination of a person's sexual orientation, such as what happened to the organisers of Queer Advocacy Week 2023, resulting in criticism and the cancellation of the event.

The findings of SAFEnet for 2023 prove that online GBV has violated people's rights to life by leading to suicide; their rights to political participation by resulting in candidates' withdrawing from electoral races; and their rights to freedom of expression and association, as happened to the organisers of Queer Advocacy Week 2023.

Part 1
Internet Access



Part 1: Internet Access

As with other public activities at the moment, the 2024 General Election cannot be separated from information and communication technology (ICT). The General Eleqtion Commission (hereafter referred to as KPU) selectively uses electoral technology [1] in its information systems. This electoral body has developed several ICT systems to support the implementation of the 2024 General Election, including the Logistic Information System (*Silog*), the Candidacy Information System (*Silon*), and the Campaign Funding Information System (*Sidakam*). [2]

The Ministry of Communication and Information (*Kominfo*) has also prepared itself for this important celebration of democracy, which comes around once every five years. Its preparations include quality telecommunication services, provision of internet access, data centres, and logistics assurance for the election. Kominfo has measured the quality of services in 514 districts and cities[3] and developed a Temporary National Data Centre (PDNS) for several applications. For example, the Information System for the Code of Ethics of General Election Implementation (*Sietik*) of the Honorary Council of Election Management Bodies (DKPP).[4] Kominfo has also collected a range of digital information to make it easier for the public to access information about the general election at https://s.id/pemiludamaipedia, consisting of several e-books and a WhatsApp chatbot.

Citizens can check the electoral roll online through the official KPU website (https://kpu.go.id) or directly at https://infopemilu.kpu.go.id or https://cekdptonline.kpu.go.id. However, there are no formal applications available for mobile devices. Only the Electoral Supervisory Board (Bawaslu) has an Android-based application, called Gowaslu, which can be used for complaints about the general election.[5]

In the context of fulfilling digital rights, the accessibility of the internet and digital technology is relevant for the public because it assists them in finding information about the election, covering everything from the stages of implementation and the mechanisms to the profiles of legislative, presidential, and vice-presidential candidates.

Access Gaps

Making information about the 2024 General Election available on the internet becomes increasingly important as the number of Indonesian citizens using the internet in their day to day lives grows. According to a survey from the Indonesian Internet Service Providers Association (APJII), internet penetration in Indonesia reached 78.19 percent in 2023, an increase of 1.17 percentage points from 77.12 percent in the previous year. There are now around 215 million internet users in Indonesia, out of a total population of 275 million people.

Nevertheless, SAFEnet's monitoring in 2023 showed that several issues relating to internet access continued to occur, including access gaps based on location and gender. A gap between rural and urban areas persists, with 64.57 percent of internet users located in Indonesia's cities. In terms of gender, men have more opportunities to access the internet

than women, with 79.32 percent of the country's men accessing the internet compared to 77.36 percent of women. Overall, the gender ratio of internet users in Indonesia is 51.19 percent men to 48.81 percent women.[6]

The availability and accessibility of the internet remained a challenge in 2023, including in the leadup to the 2024 General Election. Poor internet signal, for example, continued to be a problem in provinces like the Special Region of Yogyakarta and Bengkulu, with some residents of Gunung Kidul, Yogyakarta, unable to smoothly access the internet even though the local KPU is using *Sireka*, their digital vote counting system, in the election.[7]

In Bengkulu, around 10 percent of the province's 6,210 polling locations have internet access problems, despite the fact that the local KPU needs internet access to upload the 14 February 2024 electoral results as fast as possible. In response, Bengkulu Province KPU anticipated the need to upload data from other locations with internet access.[8]

When internet access is not even or stable, access disruptions will continue to occur. In 2023, at least 63 internet access disruptions were recorded, including 49 infrastructure-based disruptions, seven service-based disruptions, and seven policy-based disruptions.

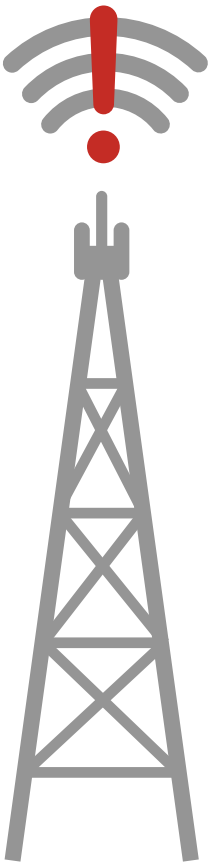


Table 1:
Total number of internet access disruptions, 2023

Aspect	Q1	Q2	Q3	Q4	Total	Dominant Issue
Infrastructure	3	16	20	10	**49**	Repeated broken cables, force majeure (nature), optic fibre cables destroyed and stolen, slowdowns/ disconnections during certain incidents.
Service	0	3	3	1	**7**	ISP service, base transceiver station service following construction, completion of the end of 3G service, disruptions to mobile applications, telco mergers.
Policy	2	4	1	0	**7**	Policies to reduce availability of public wifi, Silent Day in Bali, blocking of digital media outlets, requests for internet shutdowns in customary (adat) areas, application blocking or censorship.

Source: SAFEnet, 2024

Infrastructure

In 2023, equal distribution of infrastructure experienced a new phase. The SATRIA-1 satellite, launched in June 2023, began orbiting above Papua in the Geostationer orbit and orbiting at 146° E longitude at an altitude of more than 36,000km above earth. On 28 December 2023, President Joko Widodo formalised the construction of a base transceiver station (BTS) in Bowombaru Utara Village, Talaud, North Sulawesi. According to the Information and Telecommunication Accessibility Agency (BAKTI), this inauguration marked the end of Kominfo's 4G BTS project in Indonesia's underdeveloped, frontier, and remote areas (known as '3T' in Indonesian).[9]

Geographically, this project has been implemented in 4,991 villages, 134 districts, and 26 provinces. According to statistics,[10] the Kominfo BAKTI program was most implemented in Papua Highlands Province, where 618 BTS were built, followed by Southwest Papua Province (596 BTS) and West Kalimantan (553 BTS). Based on this data, a total of 4,988 BTS from a target of 5,618 stations were fully operating by December 2023. The remainder (630 BTS) will be constructed in 2024 due to their locations in parts of Papua with security, mobility, and force majeure challenges.[11]

Internet access disruptions were compounded by a variety of force majeure issues, both one-offs and reoccurring. For example, the undersea cable communication system in Sulawesi, Maluku and Papua in eastern Indonesia is often damaged, requiring months of repair work.[12] Breakages in this undersea cable impact internet disruptions in Papua.

Table 2:
Internet disruption incidents in Papua in 2023

Region (Dashboard IODA)	Q1	Q2	Q2	Q4	Total
West Irian Jaya (covering West Papua Province, Southwest Papua Province)	6	7	11	5	**29**
Papua (covering Papua Province, Papua Highlands Province, Central Papua Province, South Papua Province)	7	4	9	14	**34**

Source: SAFEnet, collated from IODA

Even though long distance education activities have made the digital transformation process smoother, there are still 57,223 schools not yet connected to the internet (out of a total of 274,942 schools in Indonesia, not including pre-primary school units).[13] As a result, during the Computer-Based National Assessment (ANBK), students have to go to a coastal area or to the top of a hill to get an internet signal.[14] And it was not only students in the '3T' areas with minimal infrastructure who experienced this:[15] even villages in Java, which is relatively well-developed in terms of infrastructure, students still faced connection problems.[16]

This condition was worsened by the fact that citizens are not fully aware that internet access is one of their digital rights. The public does not yet completely understand the concepts of internet speed nor the standards for quality internet speed. As a result, even though the

internet speed is often poor, the community tends to just accept the situation. And on the contrary, the Inner Baduy customary (adat) community even protested the existence of internet signal in their region, requesting that the connection be shut down.[17]

In general, citizens also have no choice but to accept the situation when their internet access speeds are problematic or slow down. In the final quarter of 2023, internet speeds in Indonesia reduced compared to the previous quarter.[18] In November 2023, Indonesia fell in its internet speed ranking, dropping to 100th position from 141 countries. Indonesia's Speedtest Global Index score showed a reduction in performance in the mobile segment, fixed broadband, and latency.

The Minister for Communications and Information acknowledged that Indonesia's average internet speed is just 22 Mbps, far below the global average of 100 Mbps.[19] Only two other Southeast Asian countries sit below Indonesia for fixed line speeds – Cambodia and Myanmar – while just Myanmar experiences slower mobile internet speeds than Indonesia.[20] Nevertheless, Kominfo itself stated that it was not appropriate to judge the average speed, remembering that Indonesia is a very large country.

Unfortunately, applications for monitoring network quality, such as the Signal Monitoring (*Sigmon*) application, have not yet been well-socialised to the public.

Services

Violations of the right to internet access in 2023 were also related to several issues of poor-quality ISP service. Even though the number of ISPs has increased in Indonesia[21] to 828 companies[22], our monitoring shows that many regions still require better services. The availability of ISPs in the '3T' areas is also minimal, as are the availability and accessibility of mobile operators.

The plans of Starlink to enter the Indonesian retail market in 2024 has spurred both the government and the private sector to provide better internet services, especially with regard to consumer price, network quality, and accessibility. This includes the retail price for end consumers and breaking down barriers to improve access in '3T' regions.

This situation has encouraged ISPs and telecommunications providers to improve their services. APJII is optimistic than the number of ISPs will continue to grow in coming years[23] in competition with businesses using low earth orbit (LEO) services. Meanwhile, the Government of Indonesia, through Health Minister Budi Gunadi Sadikin and Coordinating Minister for Maritime Affairs and Investment Luhut Binsar Pandjaitan appreciated the steps taken by foreign service provider Starlink to enter the local market,[24] although Kominfo noted they still "preferred" to optimise the SATRIA-1 satellite.[25]

Additionally, the death sentence imposed on the 3G network forced the public to shift to 4G. Unfortunately, telecommunication services following the construction of 4G BTS towers have been inadequate. For example, in Kupang District[26] and Sikka District[27], NTT. The same situation can be seen in Sumbawa District, West Nusa Tenggara (NTB)[28]; Pesisir Barat District, Lampung[29]; Tana Tidung District, North Kalimantan[30], and Jayapura District[31] and Kepulauan Yapen District, Papua.[32]

The requirement for 4G is already based in policy. However, the disconnection of networks using older technology means that the new supporting infrastructure and services must be in place. General elections also require the full participation of the community, without exception. There must be equal and quality access to 4G internet, ensuring the public has access to services relating to the election and can obtain clear information so that they can then make use of their right to vote.

BAKTI acknowledges that not all BTS can provide speeds of 25 Mbps due to Indonesia's geographical challenges.[33] Private telecommunications operators also still enforce high prices and often experience internet connection disruptions on mobile devices.[34]

Several other service issues emerge in relation to mobile banking applications, which experience technical challenges[35] and security problems[36], creating difficulties for users to access banking services. Mergers and acquisitions of local mobile telecommunications companies in Indonesia are also worth noting, as these have impacted services for subscribers.[37]

At the beginning of July 2023, Indihome merged with Telkomsel (owned by PT Telkom), leading to PT Telkom's effective ownership of Telkomsel to increase to 69.9 percent, with Singtel owning the remaining 30.1 percent of Telkomsel. Prior to that, other mergers and acquisitions in mobile telecommunications had also occurred in Indonesia. As a result, there are now only four providers of mobile internet services in Indonesia: Indosat Ooredoo Hutchinson (IOH), Telkomsel Group, XL Axiata, and Smartfren.

Policy

The post-COVID-19 pandemic digital transformation has led to massive digitalisation efforts in Indonesia. With Presidential Regulation No. 82/2023 on Accelerating Digital Transformation and National Integration of Digital Services as its umbrella policy, digital transformation and acceleration has been rolling out across the country, from procurement through to public services. This includes the information and services systems used in the implementation of the 2024 General Election.

The primary regulation regulating access rights in the digital sphere is Law no. 19/2016 *juncto* Law no. 1/2024, offered referred to UU ITE. The derivative law of UU ITE is Government Regulation no. 71/2019, known as PP PTSE, while the more technical derivative law which regulates cyber regulations is Kominfo Ministerial Regulation no. 5/2020, usually referred to as PM no. 5/2020 on Private Sector Electronic System Operators. Finally, there is Law no. 27/2023 on Private Data Protection.

In UU ITE, although there is an 'auto-blocking' mechanism for gambling content[38] and pornography, there is also a cluster of content types referred to as content which "upsets the public and disrupts public order"[39], which requires human analysis and interpretation. Meanwhile, in the policy context of election-related access, KPU Regulation no. 15/2023 through Article 37 states that voters can undertake campaigns on social media. However, this regulation only regulates the limits for the number of accounts and the campaign material, as explained in Articles 37 and 38. This is far from the main problems, which include

disruptions to information that is vulnerable to being 'misflagged' and blocked, censored, and taken down.

The impact of the auto-block policy can be seen from an incident in September 2023, in which digital services such as Google Docs, Sheets, and Slides were blocked. Screenshots taken by users confirmed that access to these services was obstructed, with errors reading "Your connection is not private". If users decided to ignore the error and continue anyway, a state-managed *'Internet Positif'* ('Positive Internet') blocking page appeared.

According to searches of the website TrustPositif, which provides a blacklist of electronic services blocked by the Indonesian government, Google Docs was indeed one of the blocked websites. The Director General of Public Communication and Information stated that they acted to restore access to the Google-owned services, saying that users had been unable to access the services not because of blocking but because of a "technical error".

Further explanation and transparency on what occurs when a website is blocked is difficult to obtain. Governance cannot only be understood as 'cyber patrols' and monitoring that are vulnerable to be ensnared in digital authoritarianism through (requests for) the blocking or removal of content. In fact, actions taken to limit access to information that are based on the Kominfo AIS crawler are prone to mistakes.[40] As a result, working with third parties such as 'trusted flaggers' is very much needed.

These notes on our observation of the right to internet access in 2023 are important as foundational input for internet governance policies following the 2024 General Election, especially as the internet has been a hot topic for the president-vice president candidate pairs. We cannot let this issue become only material for political debates, without meaningful change, especially on the right to internet access.

Part 2

Freedom of Expression

Part 2: **Freedom of Expression**

Wahyu Dwi Nugroho never expected that his TikTok content would land him in jail for five months. In fact, this father of two says he only ever wanted to share his thoughts on the erection of street-side banners forbidding locals from shopping at nearby businesses, which had impacted Wahyu's own business.

In a TikTok video made on 29 July 2022, Wahyu uploaded a photograph of a banner with a yellow background, on which was written: "WARNING! STRICTLY FORBIDDEN! Shopping at the kiosks near Al-Busyro. Punishment: You will be removed from the religious study group." Wahyu commented on the banner, writing "The best people are those who benefit those around them. [I am] very sad to read this [banner]. Our shop is not big, it only [makes] enough for our daily food and our children's education. [We] can't buy land or a house. How come they have the heart to make a banner like this?"

For his viral content, Wahyu was reported by Zakiyah, the daughter of Habib Alwi Bin Abdurrahman Assegaf, the head of the Al-Busyro *Majelis Taklim* (religious study group). The group has a large congregation, and their leadership reported Wahyu's upload to the police because they claimed they had been defamed by his content. They also stated that the content was a hoax that aimed to spark negative attitudes among the public towards the *majelis taklim*.

After being detained and prosecuted at the South Jakarta State Court, Wahyu was found guilty in August 2023. The judge stated that he had been proven to have violated Article 28 clause 2 of UU ITE on hate speech, and sentenced Wahyu to five months in jail. Even though he felt justice had not been served, Wahyu acknowledged he had resigned himself to the sentence. He was released from jail the day after the sentence was handed down, as he had effectively served the five-month period required during his pre-trial detention.

Wahyu is just one of 126 people who were reported to the police in 2023 because of their online activity. These people were considered to have committed criminal acts because they had defamed someone or had spread hate speech online. The number of people reported to the police in 2023 is a 15.9 percent increase on the previous year, when 107 people were the subject of complaints. Based on SAFEnet's observation, the 126 people were reported in 114 complaints between January and December 2023.

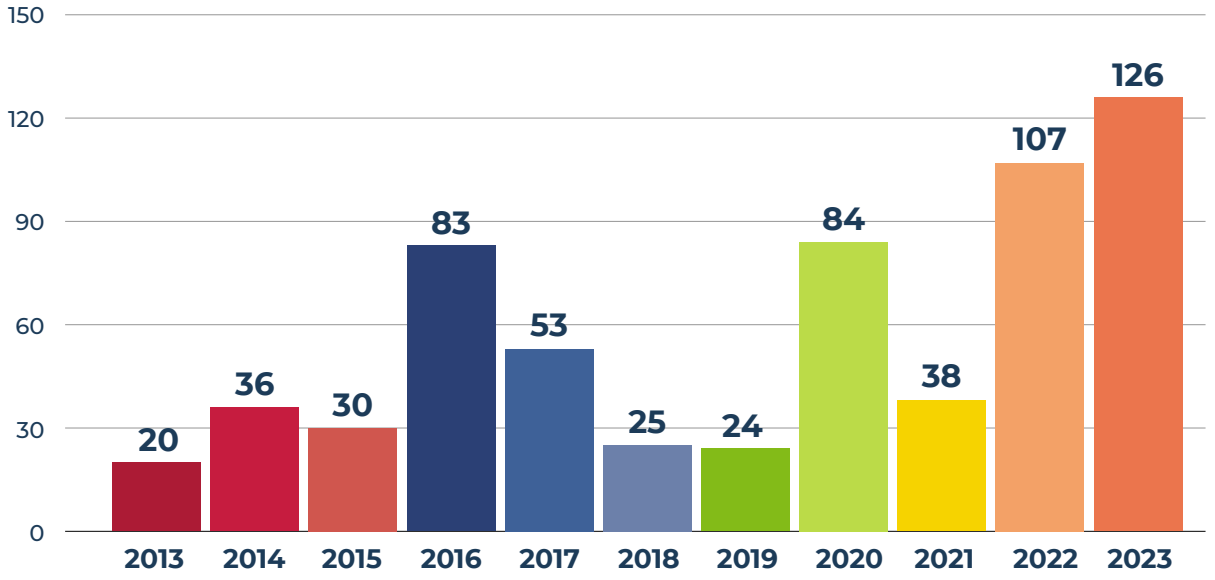
Reporting individuals to the police using criminal articles against various kinds of legitimate expression – such as opinions and art in the digital sphere – is a type of criminalisation of online expression. This criminalisation of expression limits the right to freedom of expression and opinion, which is guaranteed in Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and General Comment no. 34 on Article 19 of ICCPR. In Indonesian law, this right is also guaranteed by the Indonesian Constitution, specifically Articles 28E clause (3) and 28F, and by Article 23 clause (2) of Law no. 39/1999 on Human Rights.

Through its monitoring of and advocacy on cases of the criminalisation of digital expression, in 2023 SAFEnet continued to observe an increasing trend of criminalisation using the

problematic articles of UU ITE. This criminalisation is a serious threat for human rights because it contributes to the narrowing of civic space and democracy and encourages the practice of self-censorship among individuals and the media.

This observation aligns with the 2023 *Freedom on the Net* report, which placed Indonesia as a country where internet freedom is classified as 'partly free', with its overall score falling from 49/100 to just 47/100. This lower score was due to violations of users' rights as a result of their online activity. Other components, such as content restriction and challenges in internet access, remained the same as in previous years.[41]

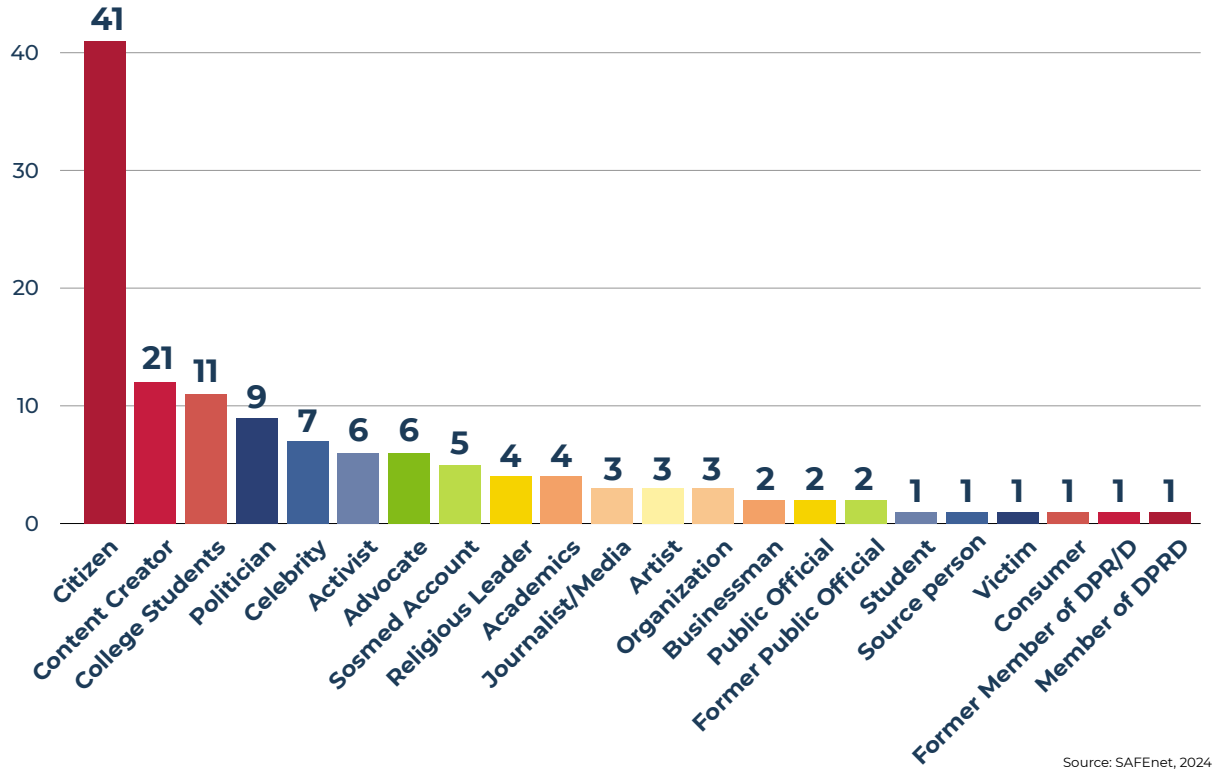
Figure 1: **Yearly Comparison of Individuals Reported in Cases of Criminalisation of Expression in The Digital Sphere, 2013-2023**



Source: SAFEnet, 2024

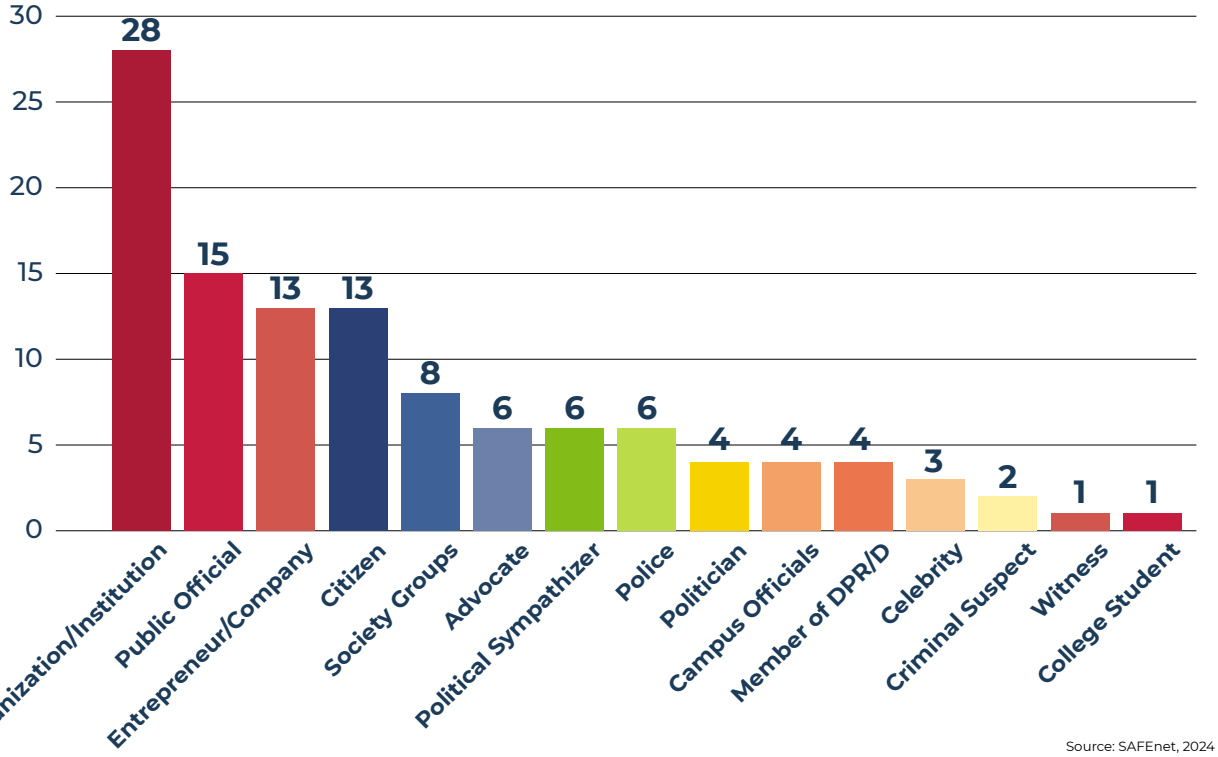
Such criminalisation is marked by power imbalances between the people making complaints and the subjects of those complaints. 2023 once again provided a clear indication of this ongoing problem. Netizens were again the most commonly reported group, alongside content creators and students, with allegations that they had violated UU ITE and other problematic articles. Meanwhile, organisations/institutions, public officials, and business people/businesses were the three groups most commonly making police reports. This illustrates the defined imbalance in the power relations between those reporting and those reported.

Figure 2: **Backgrounds of Complainants in Cases of Digital Expression In 2023**



Source: SAFEnet, 2024

Figure 3: **Number Of Complaints, Based on Backgrounds/Jobs of Those Targeted in Complaints**



Source: SAFEnet, 2024

Regulations and Articles Used in Complaints

In 2023, the use of so-called 'rubber' articles (described as such due to the 'stretchy' ways in which they can interpreted) of UU ITE were the most commonly used articles in complaints made to police, as in previous years. Almost half (48 cases, or 41.22 percent) of all cases recorded by SAFEnet in 2023 used Article 27 clause 3 of UU ITE, which regulates defamation, as the primary basis for reporting. It was not uncommon for this article to be used in combination with Articles 310-311 of the Criminal Code, which also regulate defamation.

Meanwhile, Article 28 clause 2 of UU ITE on hate speech was the second most-commonly used article, representing 28 cases (24.56 percent). Several reports using this article also used Article 156A of the Criminal Code on religious blasphemy. Another 21 complaints (18.42 percent) also simply used UU ITE as a whole, without referring to particular articles. The remainder of reports used Article 27 clause 1 of UU ITE on immoral acts, Articles 14-15 of Law no. 1/1946 on hoaxes, and Article 45 clause 3 of UU ITE on threats to disseminate electronic information that contained threats of violence.

Article 27 clause 3 of UU ITE was predominantly used by public officials (eight cases), business people/businesses (eight cases), and organisations/institutions (six cases). One example of how Article 27 clause 3 of UU ITE was used by a public official was in a case brought against Saverius 'Rio' Suryanto, a resident of Manggarai Barat, East Nusa Tenggara, who was reported to the police by the District Head of Manggarai Barat, Edistasius Endi.

Rio, a local journalist, was accused of defaming the District Head on Facebook after he uploaded several photos of the District Head which had been editing to add horns on his head and images of feet over his face. The photographs were accompanied by text-based commentary, critising the District Head of ignoring the rights of the villagers of Macang Tanggar to obtain certificates for their land.[42]

The UU ITE defamation article was also used by a business person, John LBF, to report a former employee called Septia. Septia was reported because she shared online her experience of working for 21 months at John's business, High Five.[43] In her post on Twitter, Septia stated that her bos had often cut employees' salaries without clear explanation and implemented several workplace regulations that employees considered illogical. In addition to Septia, John LBF also reported Arief Edison, the legal representative of PT Adhidharma Ekaprana, who filed a civil lawsuit against alleged fraud by High Five.[44]

Meanwhile, Article 28 clause 2 of UU ITE was mostly used by organisations/institutions (eight cases), community groups (five cases), and police/Model A reports (five cases). One case in which a community group reported an individual was that of Daniel Frits Maurits Tangkilisan, a resident of Karimun Jawa, Jepara District, Central Java. Frits opposed shrimp farming in the area because of the environmental impact on the Karimun Jawa coasts caused by farm waste. He was accused on 1 June 2023 of violating the article on hate speech, in a complaint made by a group which claimed to represent the Jepara Community Group.[45]

Table 3:
List of Regulations and Articles Used as The Key Articles in Cases of Criminalisation of Expression

Regulation and Article	Number	Percentage
UU ITE article 27 clause 3	48	42,11%
UU ITE article 28 clause 2	28	24,56%
UU ITE (no specified article)	21	18,42%
UU ITE article 27 clause 1	6	5,26%
UU 1/1946 article 14-15	3	2,63%
KUHP article 310-311	3	2,63%
UU ITE article 45 clause 3	2	1,75%
Civil lawsuit	2	1,75%
KUHP article 156A	1	0,88%

Source: SAFEnet, 2024

Platforms Used as Evidence in Complaints

Social media dominated the types of platforms or mediums used as the basis and evidence for reporting case to the police in 2023, representing 64 cases (56.14 percent). Following social media were press releases (nine cases, 7.9 percent), chat applications (seven cases, 6.14 percent), direct and actions/protests (four cases, 3.51 percent), with another five cases (4.39 percent) using other platforms as evidence. In the remainder of cases, it is not known what platforms were referred to in complaints, or that information was not included in police reports.

One interesting case involved a complaint made to the Corruption Eradication Committee (KPK) being used as the basis for a police report alleging defamation. The head of the Indonesia Police Watch (IPW), Sugeng Teguh Santoso, was accused of defamation by Yogi Arie Rukmana, the personal assistant to the Deputy Minister for Law and Human Rights, Edward Omar Sharif Hiariej. The reason? Yogi had been named in Sugeng's report to the KPK as a middleman in allegations that the Deputy Minister had received IDR 7 billion (approx. USD 443,000) in bribes.[46]

Meanwhile, several victims of criminal acts were also recorded as being 'revenge reported' to the police using UU ITE because of police reports they themselves had made. For example, a 'revenge report' was made by the family of Gregorius Ronald Tannur (GRT), who was accused of killing Dina Sera Afriyanti (DSA). GRT's family reported DSA's legal representative and family because they felt they had been defamed and their good name smeared.[47] Previously, it had been reported

Table 4:
List of Platforms Used as Evidence in Complaints

Platform	Number	Percentage
Facebook	20	17,54%
TikTok	14	12,28%
Youtube	12	10,53%
News outlet	9	7,89%
Twitter	8	7,02%
WhatsApp	7	6,14%
Instagram	7	6,14%
Direct action/protest	4	3,51%
Social media (no platform specified)	3	2,63%
Police report	3	2,63%
Comedic material	1	0,88%
KPK report	1	0,88%
Unknown	25	21,93%

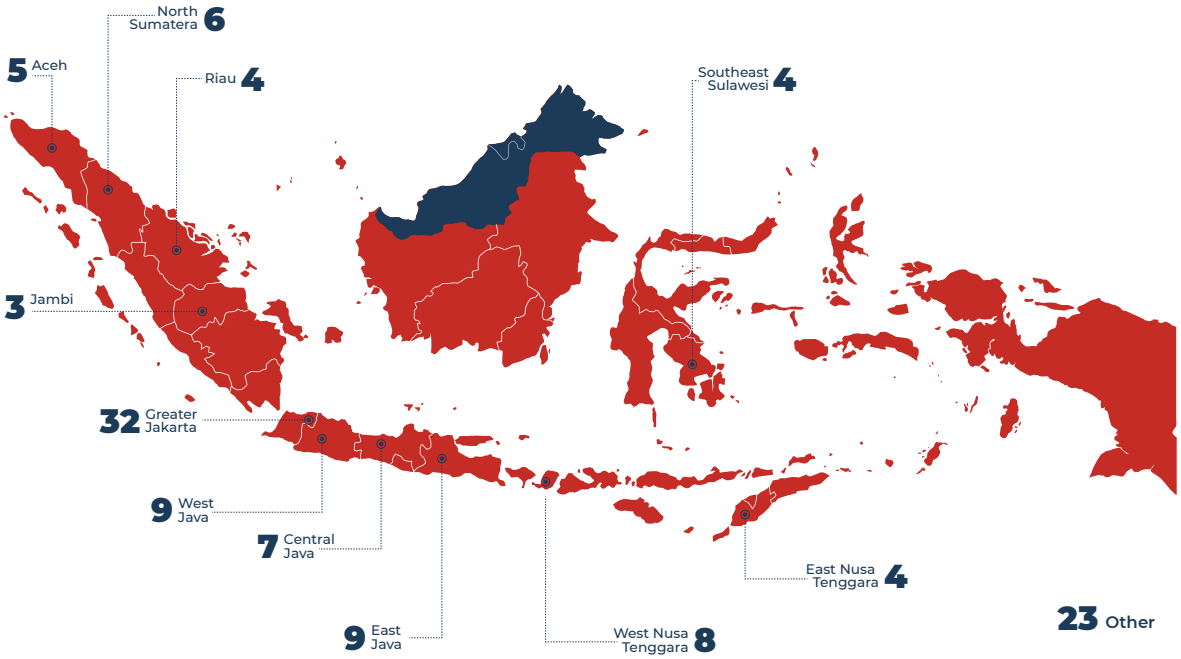
Source: SAFEnet, 2024

that DSA, a woman from Surabaya, had died after attending a night-time event where it was believed she had been physical abused by GRT.

National Spread of Cases

Criminalisation of digital expression occurred in almost all areas of Indonesia in 2023. Java remained the region with the highest number of cases, dominated by 32 reports to *Bareskrim Polri* (National Police Criminal Investigation Agency) and the Jakarta Regional Police. Police units at various levels in East Java and West Java each received nine complaints, while seven reports were made in West Nusa Tenggara. The remainder were spread across the archipelago.

Figure 4: **Number of Cases of Criminalisation of Digital Expression in 2023**



Source: SAFEnet, 2024

Politicisation of Reporting

In 2023, SAFEnet observed that there was an increase in reports made to the police with political motives in the lead up to the 2024 General Election. Political motives were identified as the second-most common reason for reporting, alongside issues of corruption, violence, and personal defamation.

Politically motivated complaints were dominated by reports made by institutions/organisations and party sympathisers, using articles of defamation and hate speech. Most of these complaints were directed at politicians and the social media accounts of ordinary netizens who shared their opinions or expressed themselves on the political conditions in Indonesia.

Based on data collected by SAFEnet, politically motivated complaints were made across Indonesia, including Greater Jakarta, North Sumatra, Central Java, Southeast Sulawesi, and

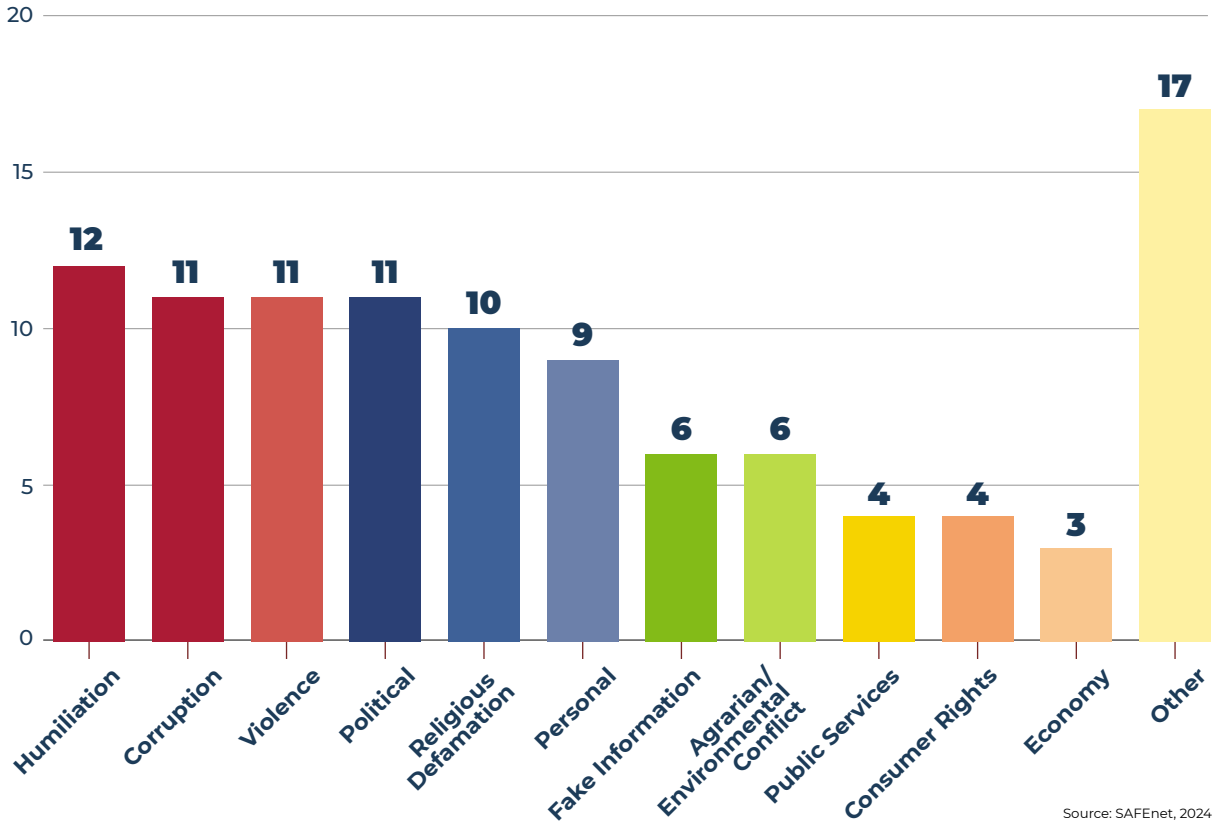
West Nusa Tenggara. At the time of writing, these complaints were still being processed by the police, so no cases had progressed to being heard in court.

One such allegation occurred in June 2023, when a volunteer for Medan Mayor Bobby Nasution reported 10 Instagram accounts to the police for allegedly spreading hoaxes. The volunteer accused the accounts of violating Article 27 clause 3 of UU ITE *juncto* Article 311 of the Criminal Code. The accounts were reported for allegedly sharing a fake video of the mayor having different attitudes towards the flags of political parties PDIP and Golkar.[48]

Article 27 clause 3 and Article 38 clause 2 of UU ITE were also used by the Head of the Solo City PDIP Branch against Margono, a member of the Solo City People's Representative Council and part of PDIP. Margono was reported to the police for smearing PDIP's name because he declared his support for the presidential-vice presidential candidate pair of Prabowo Subianto and Gibran Rakabuming Raka, even though PDIP was putting forward its own candidate pair of Ganjar Pranowo and Mahfud MD.[49]

Another complaint was made against *Koalisi Perubahan* (Coalition for Change), who put forward Anies Baswedan as their presidential candidate, by *Forum Aktivis Dakwah Kampus Indonesia* (Indonesian Forum of Campus *Dakwah* Activists, FADKI). The Coalition of Change was reported to the National Police Criminal Investigation Agency on allegations of religious blasphemy for using the abbreviation 'AMIN' as their slogan for their 2024 presidential candidate pair, even though it originated from the candidates' names: Anies and Muhaimin.[50]

Figure 5: **Motives and Issues Behind Reports Against Digital Expression in 2023**



Source: SAFEnet, 2024

Upcoming Challenges

Since 2021, efforts to revise UU ITE have been underway. Finally, the revised law was debated and ratified by the Indonesian parliament on 5 December 2023. However, this second revision of UU ITE did not align with the hopes of civil society, who had demanded a total revision of the law. The law was previously revised in 2016.

The newly revised UU ITE still contains several 'rubber' articles from the previous edition, and even gained some new problematic articles. These include articles on defamation, dissemination of hoaxes, and personal threats.

Previously, civil society had conveyed strong criticism of the closed off and secretive nature of the discussion of the draft revised law. This private debate meant that there was no meaningful public participation or role.

Consequently, as the second revision of UU ITE retains several problematic components, concerns and pessimism have emerged regarding improvements to the condition of freedom of expression in Indonesia, especially in the context of an increase in politically motivated criminalisation in the leadup to the 2024 General Election. This enables increased police reporting practices due to citizens sharing their personal expressions and opinions on the internet.

Table 5: **List of Problematic Articles in The Second Revision of UU ITE**

Article	Explanation
27A	Any Person who intentionally attacks the honour or good name of another person by accusing them of something, with the intention of making this matter known to the public, in the form of Electronic Information and/or Electronic Documents, undertaken through an Electronic System.
27B (2)	Any Person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of unlawfully benefitting themselves or another person, with the threat of defamation or the threat of disclosing secrets, forcing a person to: provide an item which partly or wholly belongs to that person or another person; or providing a loan, acknowledging a debt, or writing off a debt.
28 (2)	Any person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents that incite, invite, or influence other people so as to create feelings of hatred or enmity towards an individual and/or part of the community based on race, nationality, ethnicity, skin colour, religion, belief, sex, mental disability, or physical disability.
28 (3)	Any person who intentionally disseminates Electronic Information and/or Electronic Documents which are known to contain incorrect information that cause upset in the community.

Source: SAFEnet, 2024

Part 3

Digital Security

Part 3: Digital Security

For Anindya Shabrina, the decision to step forward as a legislative candidate was a political choice full of risk. Not only did she face scorn, she became the target of digital threats, including from her own activist friends. One of those attacks was a verbal threat uploaded to the Instagram account of a collective in November 2023: "Anin1 is what Kafka once described: Ten thousand stupid people is a political party. Don't worry about injuring a politician if you see them on the road," the comment said on Instagram.

Anindya, who was a Workers' Party candidate for the East Java People's Consultative Assembly, felt the statement was a threat targeting her, particularly because she personally knew who was behind the collective's account. She reported the post to the police, but then withdrew her complaint. Anindya had previously been the target of a police report using UU ITE in July 2018, when she was accused of defamation.

The threat against Anindya, who is also the Secretary of the Association of Victims of Internet Law (PAKU ITE), was just one example of digital attacks in the context of the 2024 General Election. Throughout 2023, SAFEnet documented at least 14 incidences of digital attacks relating to the election.

In addition to bare-faced threats on social media, like that experienced by Anindya, threats were also made through WhatsApp. This happened to the owner of the Twitter account @Neo_Historia in August 2023, who was threatened after uploading content on Twitter in recognition of Widji Thukul, a poet and People's Democratic Party activist who disappeared in 1998. Not only did they ask what @Neo_Historia's purpose was in uploading said content, the person messaging the owner on WhatsApp threatened to track them down: "I will track your location [and] destroy you all! I guarantee it!"[51]

This sort of threat – to track down someone's name and location – has also been made by sympathisers of a particular party and presidential candidate. They openly stated that they had the human resources necessary to undertake digital forensic investigation and track people. "How[ever] an account spreads hate speech, their IP address can be traced. Even to their exact location, by name, by address of their house," said Arfian, the Head of *Pasukan 08*, the volunteer body supporting presidential candidate Prabowo.[52]

The threats made against Anindya and the @Neo_Historia Twitter account may indeed remain only that: threats. Fortunately, there have not been any direct attempts to manifest these two threats. But in other cases, threats have been accompanied by digital attacks, such as those targeting the Instagram account of the Student Executive Body of Universitas Udayana, Bali, in October 2023; the WhatsApp account of Butet Kartaredjasa in December 2023; and the Instagram account of Kurawal Foundation in December 2023.

These three attacks were separate but performed in similar contexts. The Instagram account of the Universitas Udayana Student Executive Body was hacked after they posted criticism of Joko 'Jokowi' Widodo's emerging political dynasty. On 16 October 2023, they uploaded content with the title "The Politics of Loving your Children *a la* Jokowi" on

Instagram, in response to the Constitutional Court's decision on age limits for presidential and vice-presidential candidates for the 2024 election. The next day, at around 2am Central Indonesian Time, the administrator of @bem_udayana lost access to the account. The account – which had 51,000 followers at the time – suddenly logged out of all devices to which it had previously been logged in.[53]

Meanwhile, the attack against Butet occurred after the actor and comedian received a warning from the police not to discuss politics in Butet's theatre performance in December 2023. Butet felt that the warning was a form of intimidation, a restriction on artistic and political expression. "I have lost my freedom to articulate my thoughts," he said. "My freedom of expression has been inhibited."[54] One week after making this statement, Butet's WhatsApp account was hacked.

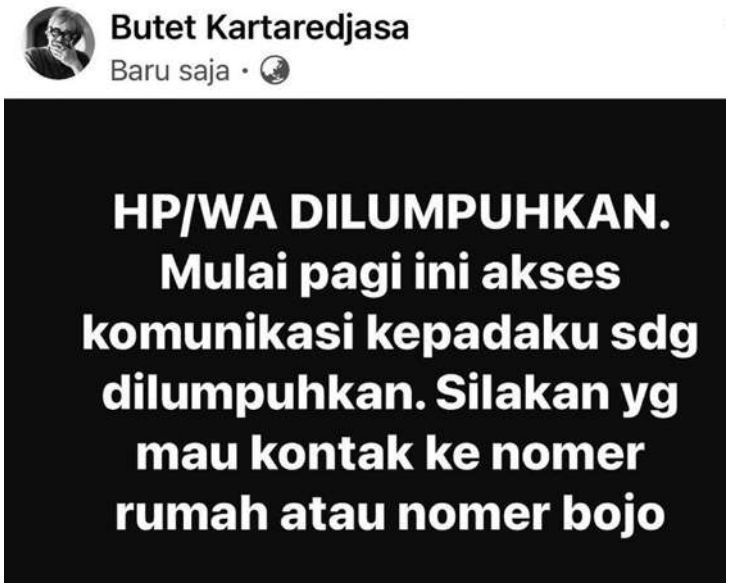


Image 1: Butet Kartaredjasa's Facebook post, stating that his WhatsApp account had been hacked. *Source: Screenshot of Facebook post by Butet Kertaredjasa, 2023.*

Then, two days after Butet's WhatsApp account was hacked, the Instagram account of Kurawal Foundation was broken into. Through Twitter, the democracy-focused civil society organisation stated that their Instagram account had been hacked. Beforehand, the foundation had uploaded content critical of one of the presidential candidates, following the first debate on 12 December 2023. The title of the content was 'Prabowo's rotten offering for Papua. The problem won't be resolved just by dancing!' Less than 24 hours after this upload, the Instagram account of Kurawal Foundation disappeared.

The administrator of the account immediately reported the account's disappearance to Meta, the company which own Instagram. The account was quickly restored. It is very likely that the Kurawal account was targeted through digital persecution – that is, through mass reporting of the account to the platform on which it appears. This form of attack has become more common recently, and includes not only mass reporting of accounts but also giving poor ratings on applications.

As The Election Neared, Attacks Increased

There are many more examples of digital attacks perpetrated in 2023 in the leadup to the 2024 General Election. All of these attacks show that as the election neared, the rate

of attacks also increased, both those of psychological nature (as experienced by Anindya and Neo Historia) and technical nature (as in the cases of Universitas Udayana's Student Executive Body, Butet, and Kurawal Foundation).

In a discussion held by SAFEnet in July 2023, a researcher from Perludem (Association for General Elections and Democracy), Nurul Amalia Salabi, stated that digital attacks indeed increase during general election periods. This occurs because general elections are political in nature and involve many stakeholders with different interests in the process and the results. The aims of such digital attacks include winning the election, causing chaos, and causing people to lose trust in the organisers, processes, and results of the election.

As a result, from the viewpoint of victims, digital attacks do not only affect critical voices, such as Kurawal Foundation, Butet, and Universitas Udayana's Student Executive Body, but also election organisers. In the leadup to the 2024 General Election, three agencies responsible for organising the election were attacked: the National General Election Commission (KPU Nasional), the Jakarta branch of KPU (KPU Jakarta), and the General Election Supervisory Agency (Bawaslu) branch in Makassar.

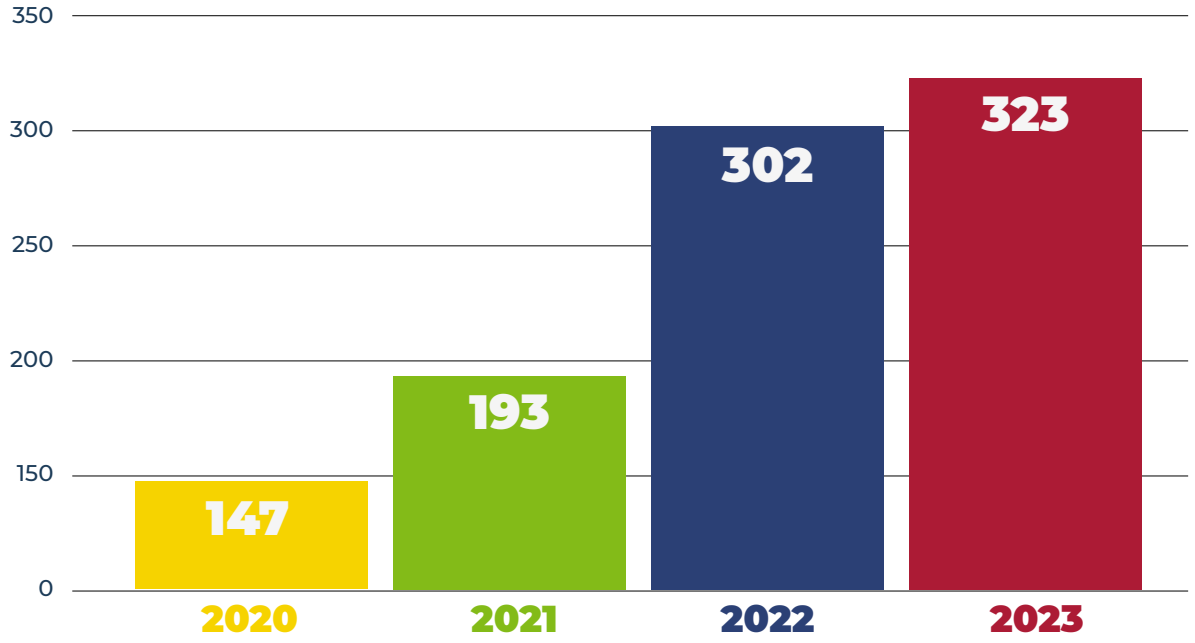
In November 2023, KPU experienced a data leak. Claiming the data came from a KPU database, a hacker sold the personal details of 204 million Indonesian citizens. This number is the exact same number as the total number of people registered on the electoral roll, which is released by KPU. As the manager of this personal data, KPU only stated that they were investigating the incident in cooperation with the National Police and the National Cyber and Crypto Agency (BSSN).[55] However, KPU did not claim any further responsibility for the incident.

Previously, in July 2023, another hacker had also offered voters' personal details for sale, claiming the data belonged to KPU Jakarta, responsible for the implementation of the election in the city of Jakarta. Meanwhile, Bawaslu Makassar experienced a different attack: the agency's website was hacked and replaced by an online gambling site. Although it was repaired, the website experienced another attack and, at the time of writing in December 2023, still could not be accessed.[56]

Reflecting on these incidents, occurring so close to the 2024 General Election, it is very likely that digital attacks will continue to increase both during and after the 'festival of democracy' is held in February 2024. This is because the data shows that digital attacks in general have increased and spread in the past five years of SAFEnet's monitoring.

Based on our observations, digital attacks and incidents in 2023 occurred a total of 323 times. This is an increase on the three previous years: 147 incidents were recorded in 2020, 193 in 2021, and 302 in 2022. Growth over the past four years indicates three things. First, our reliance on digital technology has increased, including as tools of expression and advocacy. Second, victims are more aware and more willing to report the digital attacks or incidents they experience to other stakeholders, including SAFEnet. Third, both the types of digital attacks and the victims are becoming more varied, with an array of motives present.

Figure 6: **Number of Digital Attacks Based on SAFEnet's Observations Over The Past Four Years**



Source: SAFEnet, 2024

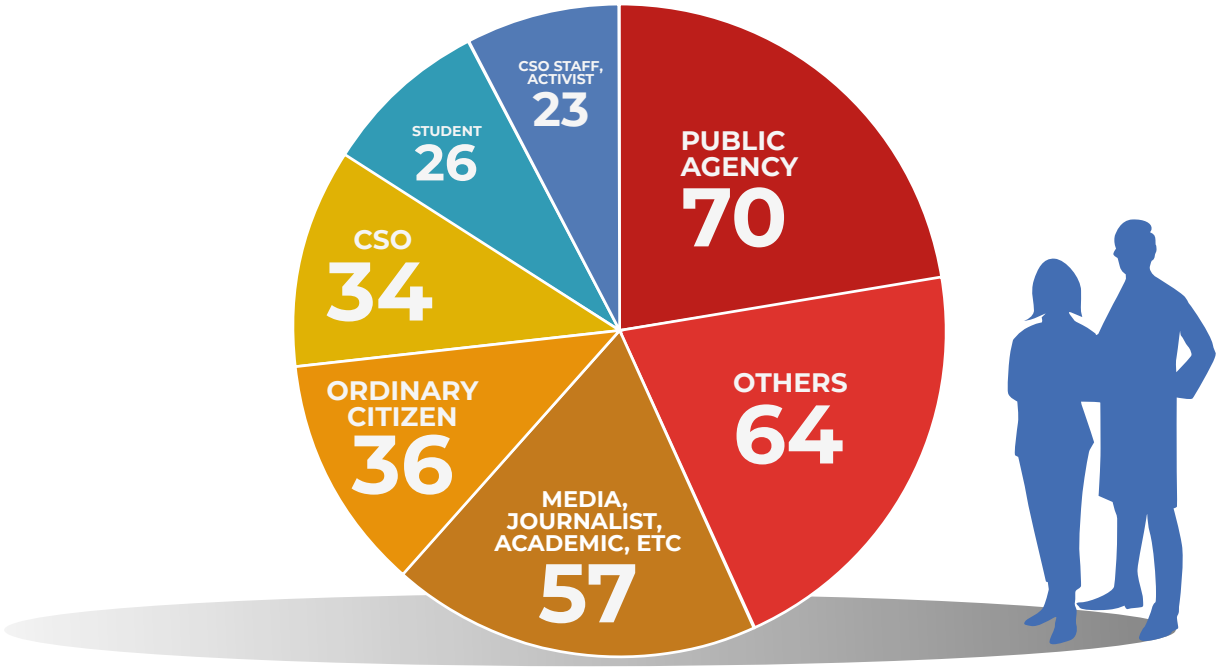
Attacks Continue to Spread

The number of digital attacks in 2023 varied from month to month. The highest number of attacks occurred in June, when 94 attacks were recorded, followed by May (51 attacks) and August (36 attacks). It was only in February and April that less than 10 cases were recorded, with seven and two attacks documented respectively. On average, 27 digital attacks and incidents occurred every month. The high number of digital attacks in July and August 2023 was primarily as a result of systematic attacks using Android Package Kit (APK) files spread on WhatsApp groups of ordinary citizens, students, and Papuan activists. Installed on Android devices, the APK files resulted in perpetrators being able to access users' messages and internet activity.[57]

In terms of who the victims were, digital attacks most often targeted public agencies, representing 21.67 percent of incidents. This is the same as in previous years, when public agencies also experienced multiple data leaks being bought and sold on the dark web or hackers' forums, including data from KPU. In second place, digital attacks also targeted ordinary citizens (11.15 percent).

Even though the number of attacks decreased, incidents continued to target critical voices, such as activists, journalists, media outlets, and civil society organisations (CSOs). In 2023, digital attacks against activists and CSO staff occurred 23 times (7.12 percent). Meanwhile, digital attacks targeting journalists and media workers were recorded 12 times (3.7 percent), with media outlets themselves being affected 15 times (4.64 percent). If combined, SAFEnet's findings show that there were 27 digital attacks (8.36 percent) against journalists and the media in 2023.

Figure 7: **Victims of Digital Attacks in 2023 Based on Identity and Work**



Source: SAFEnet, 2024

Digital attacks against the media targeted mainstream media outlets as well as non-profit and independent outlets. Mainstream media attacks included attacks against the Twitter account of Suara in July 2023, whose account was suddenly unable to be accessed after the outlet had been intensively uploading content relating to their collaborative news coverage of the use of tapping devices such as Pegasus in Indonesia. Other media outlets which experienced digital attacks in 2023 included Project Multatuli in August and Kompas.id in December. The two outlets were attacked through DDoS attacks, flooding their websites with bots to cause the websites to become inaccessible.

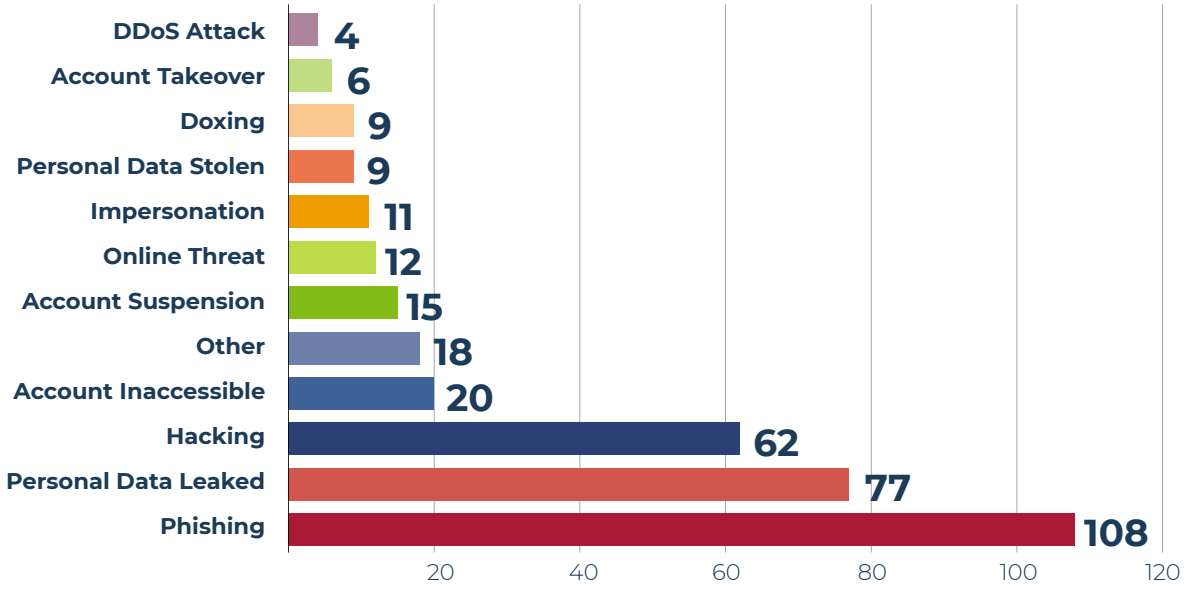
Digital attacks against journalists and the media also spread further in 2023. According to SAFEnet's observations, digital attacks also targeted independent media outlets, including puankhatulistiwa.com in Pontianak, West Kalimantan; FLoresa.co in Flores, NTT; and BaleBengong.id in Denpasar, Bali. These three outlets are non-profit in nature and focus on public issues in their respective regions.

One journalist who experienced digital attacks was Manfred Kudiai, a journalist with The Papua Journal. Manfred was attacked online after he covered the trial of Victor Yeimo, who was accused of treason.[58] During his coverage, officials demanded that Manfred and his acquaintances hand over their mobile phones and cameras. After initially refusing, they agreed to surrender their devices. Several weeks after the trial, Manfred's main Facebook account – which he used to share his coverage – could not be accessed, even though Manfred had implemented two factor authentication (2FA) on the account. Despite his security strengthening attempts, Manfred still became a victim of digital attacks.

Types of Attacks

The most common form of digital attack documented in 2023 was in the form of phishing (links with malware). This was recorded a total of 108 times (32.73 percent). In second and third place, respectively, were personal data leaks (77 incidents, 23.33 percent) and hacking (62 incidents, 18.79 percent). Three other forms of digital attacks were also recorded in 2023: accounts suddenly inaccessible (20 incidents, 6.06 percent), suspension of accounts (15 times, 4.55 percent), and threats (12 incidents, 3.64 percent).

Figure 8: **Types of Digital Attacks in 2023**



Source: SAFEnet, 2024

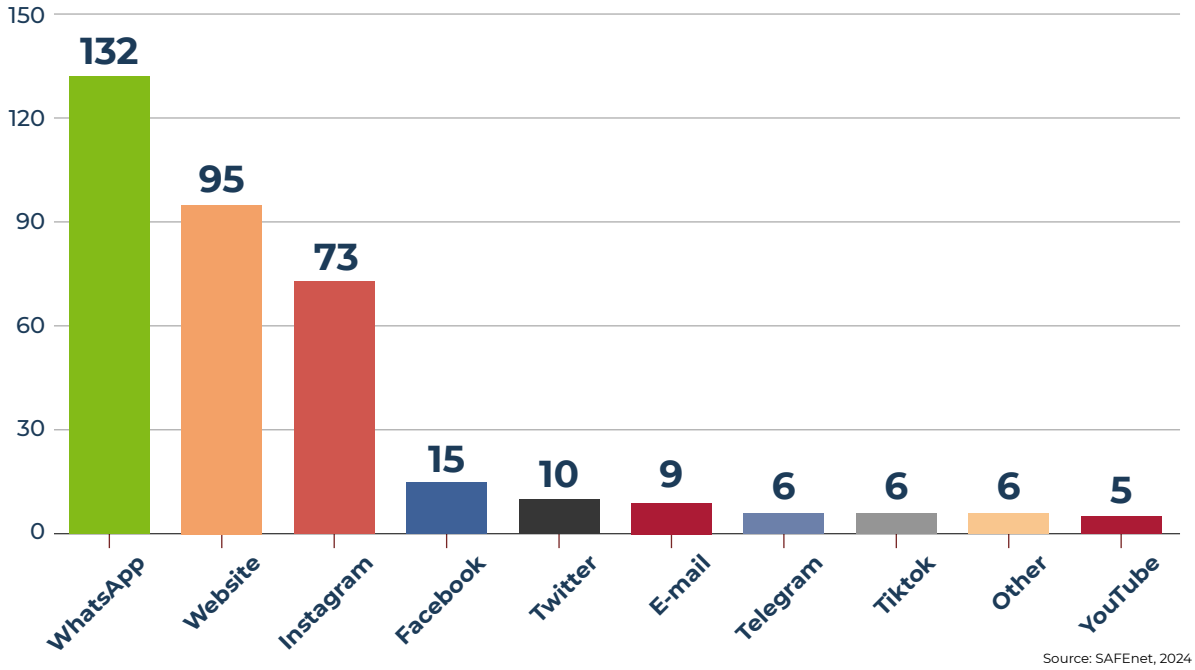
Widespread phishing attacks in 2023 primarily used the two most popular platforms in Indonesia: WhatsApp and Instagram. On WhatsApp, phishing was implemented through sending APK files, such as to groups of ordinary citizens, students, and Papuan activists. Most commonly, though, ordinary citizens were targeted. This method of attack emerged in 2022 and continued in 2023. Victims of phishing even included senior police officials, such as the Head of Central Java Police, Inspector General Ahmad Lutfi, who received a WhatsApp phishing messages with an APK file in July 2023. He opened the file without thinking, enabling the perpetrator to remotely control his mobile phone. Not long after, two perpetrators were detained.[59]

Two types of digital security incidents and attacks were increasingly witnessed in 2023: accounts suddenly becoming inaccessible, and accounts being suspended. If we combine these two categories, at least 35 incidents took place in 2023. When accounts become inaccessible, there is rarely any reason provided; suspensions, on the other hand, usually give information from Meta that the account has been suspended. Meta most commonly informs the user that the account has violated its community guidelines.

In 2023, account suspensions affected university-based groups and LGBTIQ groups. In March 2023, the Instagram account of Girl Up UGM (@girlup.ugm, based at Universitas Gadjah Mada in Yogyakarta) suddenly became inaccessible due to activity considered not

in line with community guidelines. The same thing happened to the Facebook page and Instagram account of Suara Kita, a LGBTIQ community, who could not upload links to their website in May 2023. They received a message explaining they had violated the community guidelines, although it was not clear how.

Figure 9: **Platforms Targeted by Digital Attacks in 2023**



Source: SAFEnet, 2024

Platforms Most Attacked

Meta-owned platforms were the most commonly attacked in 2023. SAFEnet's observations found that Meta's platforms – consisting of Instagram, WhatsApp, and Facebook – experienced at least 220 digital attacks (61.62 percent). Other platforms included websites (132 incidents), Twitter (10 incidents), email (nine incidents), Telegram (six incidents), TikTok (six incidents), and YouTube (five incidents).

Attacks perpetrated through WhatsApp affected the activists behind the weekly Thursday protests, known as *Kamisan*, in Medan, North Sumatra, in February 2023. At least five activists were targeted at the same time, rendering their WhatsApp accounts inaccessible. Prior to the hacking, several activists were approached by the police, who had asked them to cancel their *Kamisan* protest because President Joko Widodo would be visiting the area.

WhatsApp-based attacks also targeted four activists from *Jaringan Advokasi Tambang* (Mining Advocacy Network, JATAM) in May 2023 and leaders of Amnesty International Indonesia (AII) in August 2023. Meanwhile, Instagram-based attacks affected the accounts of *Aliansi Jurnalis Independen Indonesia* (Indonesian Independent Journalists' Alliance); *Balairung*, the student press of Universitas Gadjah Mada, Yogyakarta; and Kurawal Foundation.

In 2023, six reports were also made about attacks implemented through TikTok, while attacks also increased on the Google-owned platform YouTube. Even the official People's Consultative Assembly's official YouTube account was attacked in September, several months after the account of the Welfare and Justice Party (PKS) was attacked in January.

In several cases, these digital attacks were not only perpetrated through a single platform, but used several platforms at once. This was the experience of independent media outlet Floresa.co in May 2023, who were attacked on three platforms (Telegram, WhatsApp, and their website) following the publication of a report criticising the ASEAN Summit held in Labuan Bajo, Manggarai Barat, Flores. The attacks against Floresa.co further strengthen the evidence that digital attacks in Indonesia are becoming more political and are spreading to more parts of the country.

Part 4
Online Gender-based Violence

CONTENT WARNING:

This section contains content about suicide and online gender-based violence, which may cause readers to feel uncomfortable or spark traumatic responses.

Continue, or pause reading if you feel uncomfortable, and return later when you feel prepared.

Part 4:
Online Gender-based Violence

When her intimate personal video went viral online, MRRH's hopes for the future fell apart. A female politician from NTT, MRRH was preparing to stand for election as a legislative candidate in NTT. However, someone made and uploaded a video of MRRH without clothes and spread it online through WhatsApp, Twitter, and Facebook.

The viral video showed MRRH wearing her Nasdem Party uniform, with text stating her polling number: Legislative Candidate No. 4. Then, the video showed MRRH without clothes. The video lasted for only 21 seconds, but it destroyed MRRH's career as a young female politician from Eastern Indonesia.[60]

In August 2023, six months before the 2024 General Election, MRRH withdrew her candidacy. She also resigned as a member of her party, Nasdem, even though her name was already on the Draft Candidate List issued by the NTT branch of KPU as a candidate for Electoral Area 1, including Kupang City, the capital of NTT.

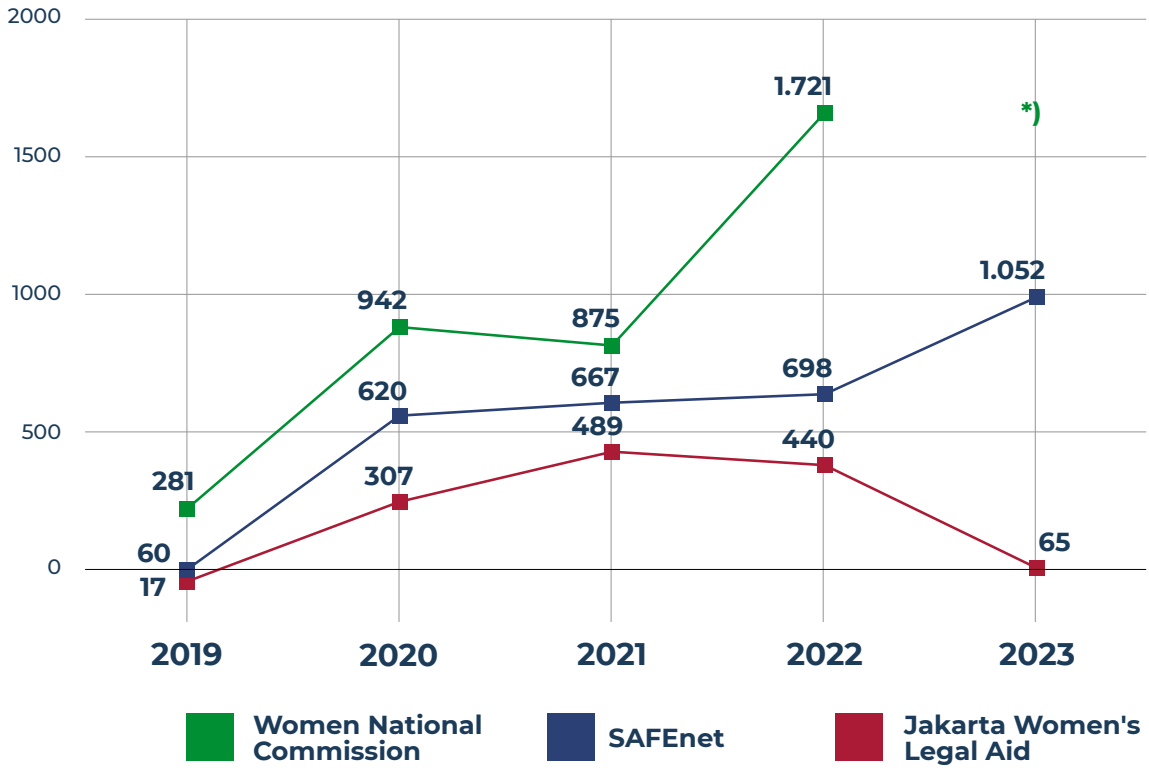
Although MRRH had to end her political career, at least until after General Election 2024, another young woman in the same province took an even more extreme path after a similar experience: suicide. PN, a 16-year-old girl from Timor Tengah Utara District, killed herself after her intimate content was spread on social media by someone she knew, FB.

FB and PN were actually related. FB pretended to be PN's boyfriend, VS, and asked for intimate photos of PN through Facebook.[61] After obtaining a video 15 seconds in length, FB shared it to PN's school's Facebook group. The video – which PN had intended only for her boyfriend – went viral and became the talk of the school. PN was ashamed, and chose to end her life, even filming the moment she did so.

The Timor Tengah Utara District Police investigated VS, FB, and four witnesses who were members of PN's school Facebook group. However, there has not been any public updates about the results of the investigation. All we are left with is a demonstration of how online GBV has taken away the futures of young women like MRRH and PN.

Looking at the situation from the perspective of the 2024 General Election, we can see that online GBV can be used as a political weapon to attack an individual's electability. The story of MRRH is just one example. Election-focused organised Perludem found that psychological attacks against electoral participants and observers were common throughout election periods.[62] These psychological attacks are particularly experienced by female and gender minority politicians to intimidate them by sparking public hatred. One narrative often used in this way is individual politicians' support for the LGBTQ community. This is perpetrated not only to win electoral contests, but also to destroy the public's trust in the political process and general elections, as well as to arouse feelings of hatred.

Figure 10: **Comparison of Online GBV Complaints at Three Service Providers**



*) National Commission on Violence against Women is not Publish 2023 Report yet Until January 2024

Source: LBH APIK, Komnas Perempuan, & SAFEnet, 2024.

Number of Victims Keeps Growing

Although online GBV has been occurring in the context of the 2024 General Election, we cannot ignore the 1,052 complaints of online GBV received by SAFEnet in 2023. Online GBV – sometimes referred to as technology-facilitated violence against women (TF-VAW) and gender-based cyber violence – has opened up a new space for violence, and used by perpetrators for a wide range of interests.

SAFEnet is not the only institution who receives reports of online GBV. Other institutions include the Women's Legal Aid Body (LBH APIK) and the service provision unit of the National Commission on Violence against Women (Komnas Perempuan). Over the last three years, complaints to Komnas Perempuan have increased annually.[63] Complaints made to SAFEnet have also increased from year to year: from 677 reports in 2021 to 698 reports in 2022, and reaching 1,052 complaints in 2023 (an increase of 33.65 percent). The most complaints were receive in July 2023, when a total of 120 online GBV reports were made.

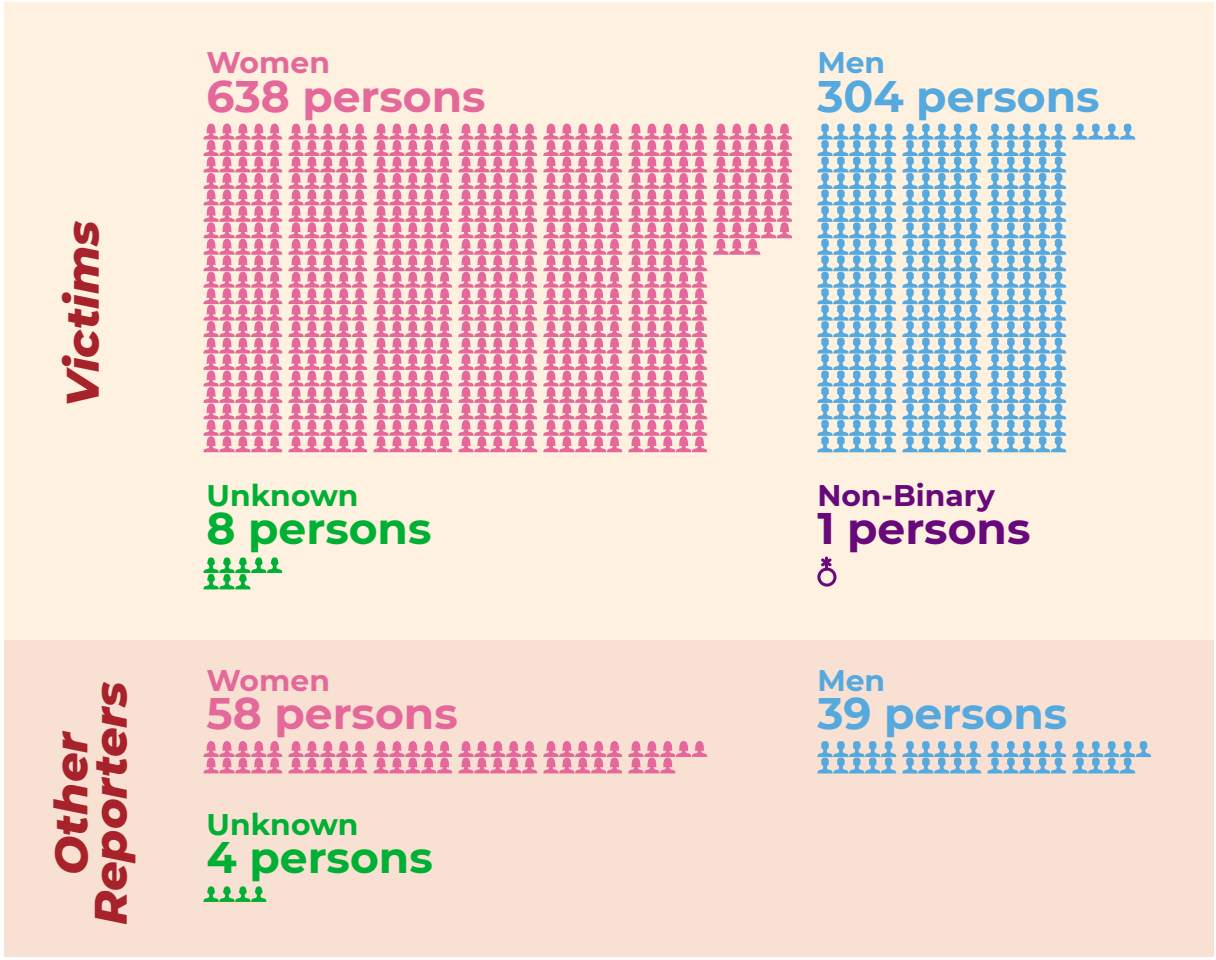
The high number of reports may be for two reasons. First, more people are becoming aware of online GBV and its dangerous nature. Second, there is increased trust in support services, including SAFEnet. These two factors indicate the same thing: that cases of online GBV are increasing from year to year.

Who is Reporting Online GBV?

SAFEnet receives reports of online GBV through its platform at https://aduan.safenet.or.id. Of the 1,052 complaints SAFEnet received in 2023, 951 were made by victims themselves. The remaining 101 reports were made by representatives of victims, including friends, family members, and supporters.

In terms of gender, 638 of the victims were female, 304 were male, and one was non-binary. This shows that online GBV can be experienced by people of all genders and sexualities.

Figure 11: **Who Reported Online GBV in 2023 (gender-disaggregated)**



Source: SAFEnet, 2024

In terms of location, West Java saw the highest number of reports made, with 243 incidents. Next highest were East Java (128 reports) and Jakarta (122 reports). Outside Java, East Kalimantan contributed the most reports with 16, followed by Bali (11), South Sulawesi (eight), and West Kalimantan (eight). Two reports of online GBV also came from Papua. As ICT access improves in more areas, the potential for online GBV also increases. This emphasises the urgent need for building digital literacy on online GBV prevention across the country.

In terms of age, from 1,052 reports, a total of 562 reports (53.42 percent) were reported by online GBV victims aged between 18 and 25 years old. Close attention should be paid to children in the 12-17 age group, as 230 cases (21.87 percent) were reported. Other people

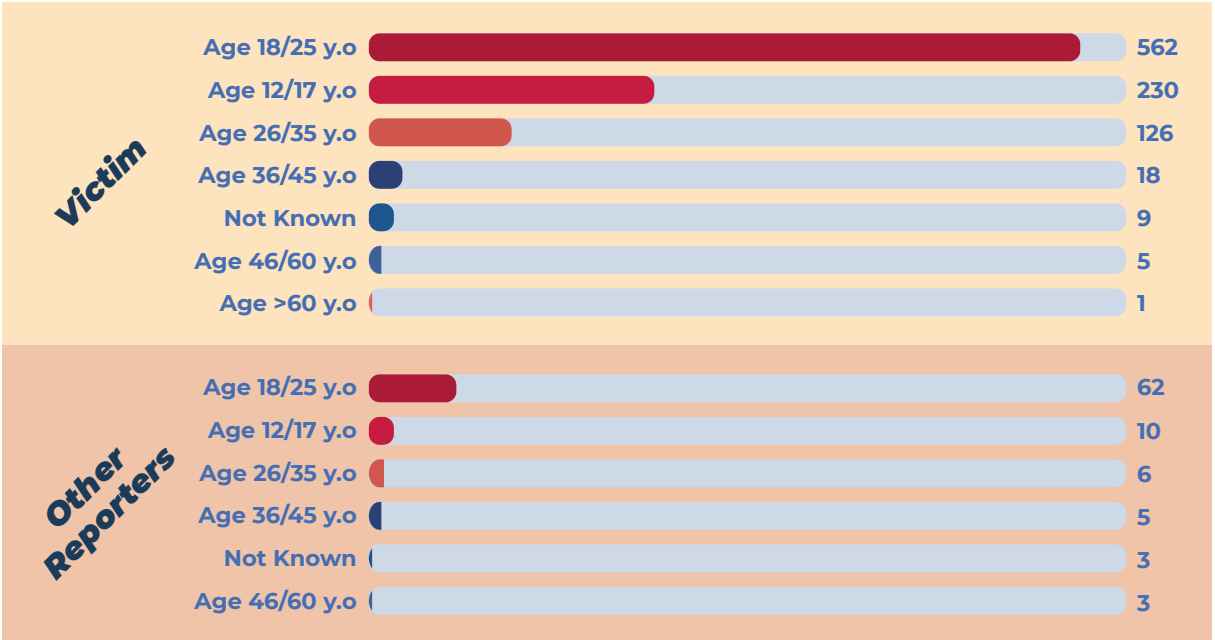
making reports of online GBV against children represented 10 cases (1 percent).

Figure 12: **Location of People Reporting Online GBV in 2023**

Source: SAFEnet, 2024

The increasing number of children experiencing online GBV requires special attention, as from year to year, this situation is not improving. Child protection agency ECPAT found that child sexual exploitation happens on big social media platforms such as those owned by Meta.[64] We must increase our efforts towards child protection in the digital sphere: not only do we need to teach digital literacy, we also need to improve monitoring and prevention efforts in all state policies and ensure they are properly implemented by law enforcement agencies.

Figure 13: **Age of People Reporting Online GBV in 2023**

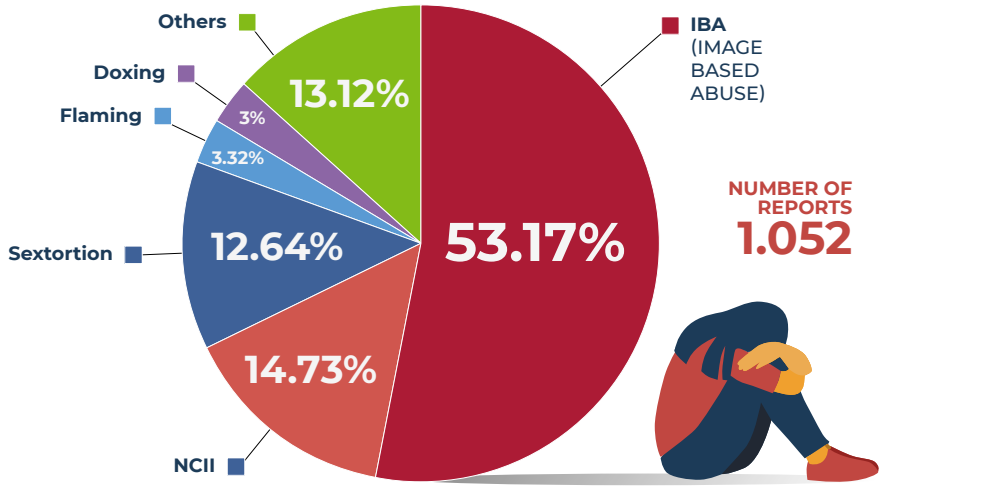


Source: SAFEnet, 2024

Types and Impacts of Online GBV

The most commonly-experienced type of online GBV reported to SAFEnet was image-based sexual abuse (IBA), in which a victim's intimate content is misused, which made up 53.13 percent of 1,052 complaints. This was followed by non-consensual intimate image (NCII) abuse at 14.73 percent, sextortion at 12.64 percent, flaming at 3.32 percent, and gender-based doxing at 3 percent. Other forms of online GBV to which more attention should be paid include the creation of impersonation accounts, outing someone's sexual orientation, and account takeovers, which were experienced by less than 2 percent of people reporting cases in 2023.

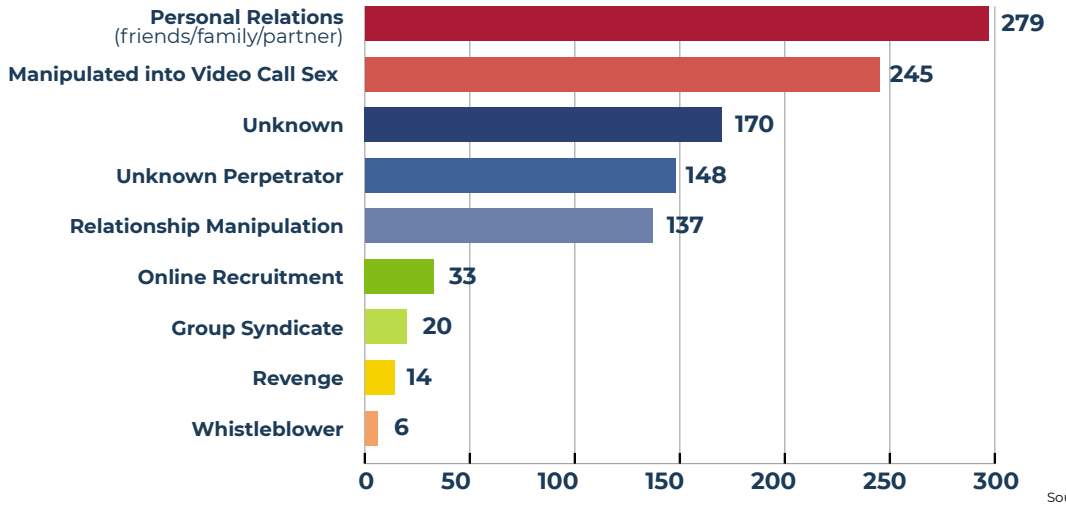
Figure 14: **Types of Online GBV Experienced by Victims in 2023**



Source: SAFEnet, 2024

SAFEnet also received reports about blog sites which contained intimate content involving victims manipulated into participating in 'video call sex' (VCS).[65] This form of online GBV is becoming more common, and includes both threats from individual perpetrators and systematic threats from syndicates. Manipulation of VCS also affects child victims. Of the complaints made to SAFEnet,[66] perpetrators tend to lure victims into participating in sexual activity by contacting child victims first. The victims are then shown pornographic content while being recorded and encouraged to perform sexual activity.

Figure 15: **Modes of Online GBV in 2023**



Source: SAFEnet, 2024

In terms of impact, the impacts of online GBV vary significantly. In extreme cases, such as the one mentioned earlier, the victim committed suicide. In other cases, victims often isolated themselves from the threats and viral intimate content being spread by the perpetrators. Some victims reported being encouraged by perpetrators to kill themselves. "The perpetrator told me to kill myself. After that, he sent my disgraceful photographs, downloaded all the photographs of my family, and threatened he would destroy me and my family," reported a victim who was threatened in November 2023.[67] This victim's experience shows how online GBV can take away victims' mental and psychological ability to continue participating in their life in the offline world.

Online GBV has also stolen victims' digital rights. Perpetrators' efforts to threaten individuals can cause victims to stop using the internet. Alongside this, digital attacks that occur in a variety of forms of online GBV can also make it difficult for victims to think and express themselves online. In other words, online GBV impacts the equality and inclusivity which should be present in our digital rights.

The Forgotten Digital Rights of Vulnerable Groups

Digital rights which fulfill the requirements of being equal and inclusive – such as access for sexual minorities, people with disabilities, Indigenous groups, women, children, and Papuan people – are still not accommodated in Indonesia. The increase of content moderation, prohibition efforts, and internet infrastructure from the Government of Indonesia remain at the level of internet restrictions and account takedown in the public interest.

Remotivi, SAFEnet, LBH Masyarakat, Arus Pelangi, and Sanggar Swara, in their 'Being Queer on the Internet' ('Menjadi Queer di Internet') publication, summarised the digital rights challenges faced by vulnerable groups. Identified problems included around the right to internet access, the right to digital security, and the right to freedom of expression.

In terms of the right to internet access, the publication found that vulnerable groups' access problems are economic and infrastructure in nature. The internet has not yet become a fundamental need for vulnerable groups.[68] In addition, in regard to the rights to digital security and freedom of expression, vulnerable groups continue to have their access and content restricted, such as what happened with the internet shutdowns in Papua and the blocking and removal of content, websites, and platforms used by Papuans and LGBTQIA+ people.[69] These situations were made worse by attacks targeting the accounts of other vulnerable individuals and groups.

It is not an insignificant number of vulnerable groups who experience online GBV both directly and indirectly. For example, one social media platform busily discussed a post outing people's health statuses, where the perpetrator who outed others was a health worker in West Java.[70] The organisers of Queer Advocacy Week 2023 were also outed then criticised for cancelling the event.[71]

These acts were responded to by several parties, including the Alliance of Independent Journalists of Indonesia (AJI Indonesia). "Arus Pelangi [an LGBTQ+ NGO] constantly received death threats through its Twitter and Instagram accounts. The buzzers and influencers are

fuelling hatred [towards them]," AJI Indonesia said in its press release.[72] The outing and doxing efforts targeting the Queer Advocacy Week organisers show that online GBV can also take away people's freedom to gather and associate, including attacking individuals from vulnerable groups.

Image 2: Online petition demanding cancellation of Asean Queer Advocacy Week 2023.
Source : petisionline.com

Meanwhile, disability groups experienced other challenges. KPU has been optimistic in its ability to hold General Election 2024 in a way which fulfils the rights of people with disabilities. The rights included here include the right to enrol as a voter, the right to information on the general election, and the right to accessible voting locations. However, even in the leadup to the election, access to information about it remains insufficient.

For Deaf people, the presidential candidate debate was made accessible through the provision of a sign language interpreter. However, on people's TV screens, the lower right-hand box presenting the interpreter was too small and sometimes covered by advertising, while no closed captions were made available to help Deaf people understand the debate. In comparison, Surya Sahetapy, a Deaf man, provided a screenshot of the presidential debate in the United States between Donald Trump and Joe Biden, in which two sign language interpreters were shown throughout the debate. Two sign language interpreters were used so that every time one of the candidates spoke, they had a dedicated person to interpret their speech into sign language.

Meanwhile in Indonesia, only one sign language interpreter was present, meaning they must interpret the speech of all candidates. Surya Sahetapy argues that KPU should, in fact, provide four interpreters – one for each of the three presidential candidates and one for the moderator – and add closed captions in the Indonesian language.

This recommendation could be easily implemented, as proven by Deaf organisation Gerkatin, who recorded re-broadcasts of the presidential and vice presidential debates on their YouTube channel. These re-broadcasts provided larger boxes for the sign language interpreters, used four interpreters, and provided Indonesian closed captions, ensuring that Deaf people can fully access the information.

A Fresh Breeze in The Midst of Challenges

In the midst of online GBV threats, legal efforts are not always blunted. The Sidoarjo State Court[73] ruled that the perpetrator was guilty in a 'creepshot' case[74] by considering the phrase "recording, taking photographs, and capturing screenshots which are sexual in nature" in the Sexual Violence Offences Law (UU TPKS). This ruling is an example of good practice on handling cases of online GBV in Indonesia.

However, the fresh breeze spurred by the Sidoarjo State Court's use of the Sexual Violence Offences Law highlights just how the Law has not yet been fully implemented in Indonesian law. Many law enforcement officers do not yet understand how to use the Sexual Violence Offences Law and are reluctant to use it due to the lack of implementing regulations. One of these missing implementing regulations should cover management of content containing electronic sexual violence.

This regulation is referred to in Articles 46, 47, and 55 of the Sexual Violence Offences Law, where it is stated that content containing electronic sexual violence is the responsibility of the central government and judiciary. However, provisions on takedowns of such context are to be further regulated by a Government Regulation (*Peraturan Pemerintah, PP*).

Ideally, regulations on management of content containing electronic sexual violence should fulfill the digital rights of victims. Several civil society organisations – including SAFEnet, Institute for Criminal Justice Reform (ICJR), Purplecode, LBH APIK Jakarta, *Kolektif Advokat Keadilan Gender* (Advocates' Collective for Gender Justice), and Jakarta Feminist – collaborated to develop recommendations in a policy paper to encourage this.[75]

These recommendations include, among others, suggest the expansion of the definition of electronic sexual violence; clear lines of responsibility and coordination for the takedown of content containing electronic sexual violence; and foundations for the strengthening of fulfilment of victims' fundamental rights, such as the right to be free from torture, cruel, inhuman and degrading treatment or punishment, and the rights to freedom and safety. In addition, the policy paper recommends capacity building of civil society organisations, victim support institutions, and ground-level implementers who can request takedowns of sexually violent content. Multi-sector coordination in content removal should heed checks and balances in all agencies. Other elements which require regulation include content removal and the right to be forgotten which prioritise the victims.

Efforts to protect digital rights must also be held in high esteem when it comes to content management, especially in the context of vulnerable groups. Content moderation undertaken by the government must fulfil the requirement to protect victims of online GBV as well as the access of vulnerable groups, rather than acting single-handedly in 'the public interest'.

Epilogue

Epilogue

Pemilihan umum telah memanggil kita,
Seluruh rakyat menyambut gembira.

The general election is calling us,
The whole community greets it happily.

The lyrics of the election march written by Mochtar Embut in 1971 do not feel relevant anymore if we look at the current conditions. Rather than being greeted with happiness, the most recent elections have instead made people cautious. It is not surprising to see comments like "I hope the 2024 General Election will be over soon" all over social media; these comments reflect the public's embarrassment over the increasing amounts of political drama that emerge as we approach the 2024 'festival of democracy'.

This embarrassment is well-reasoned, however, noting the high number of cases of digital attacks and criminalisation relating to the election. The Election Vulnerability Index developed by Freedom House highlights the challenges that undermine the integrity of the 2024 General Election in Indonesia. With a score of 58 out of 100, Indonesia is rated as having significant homework on the legal front, the physical safety front, and equal treatment.[76] Other challenges are present in terms of digital content restriction on political and social issues, alongside the presence of regulations which punish people for their online activity.

Freedom House also analysed the increase in digital election disturbances over the last few years in its Election Watch in the *Digital Age* publication. The trend emerging in this report showed that there has been a series of efforts to control the digital world in the leadup to general elections. For example, the unleashing of cyber attacks and the blocking of access to independent news websites, the detention of internet users for their political opinions, the ratification of repressive regulations, the dissemination of disinformation, and the restriction of the internet and communication. These trends were also witnessed in the 2019 General Election, such as when state agencies responsible for the implementation of the election were hacked and experienced data leaks.

Learning from the experiences of 2019, democracy NGO Perludem have highlighted the importance of anticipating cyber attacks in the 2024 General Election. Perludem underlined the importance of KPU and Bawaslu in ensuring the digital security and 'cleanliness' considered crucial. These agencies, which benefit from using an array of digital technologies, must be capable of avoiding cyber attacks like the ones of 2019.

The Community Advocacy and Study Institution (*Lembaga Studi dan Advokasi Masyarakat, ELSAM*) have also presented several digital threats and risks which can seriously impact the process and integrity of the 2024 General Election. For example, the potential for an increase in the number of eligible voters who decide not to vote because of concerns about the exploitation of voter data; the presence of a culture

among election implementers which ignores security and data protection risks; and the other dangerous impacts of cyber security attacks and exploitation of voters' personal data.

This growth in election disturbances is also intertwined with digital rights violations that become increasingly evident as voting day approaches. These practices are unlikely to cease even if the country elects a new leader, whoever they may be. It is like falling down, only to be hit by a ladder as well. 'Concerning' is the word which can describe the unfortunate condition facing the Indonesian people right now.

Data collected by SAFEnet over the past five years shows that the political momentum in Indonesia has actually fed digital rights violations. Restrictions to internet access, criminalisation of expression, digital attacks, and politically-motivated online gender-based violence continue to occur and have become a serious and realistic threat to the public. This phenomenon shows that the types of repression facilitated by technology have become effective instruments in controlling narratives and silencing critical voices.

The situation is exacerbated by the absence of a digital rights perspective in the visions, missions, and programs of the presidential and vice-presidential candidates competing in the 2024 General Election. Even though the words 'internet' and 'digital' appear in the candidates' campaign documents, digital rights are not manifested in their track records. In fact, one candidate pair even made fun of the free internet program promised by another candidate pair, even though affordable and accessible internet is part of the public's digital rights, which must be fulfilled by the state.

Several candidate pairs have mentioned their intentions to revise UU ITE again, as this Law is considered a threat to freedom of expression in Indonesia. However, ironically, the parties behind these candidates were actually part of the efforts to ratify the controversial second revision of UU ITE. Not only that, party sympathisers and candidate supporters continue to report one another to the police using articles from the repressive UU ITE.

Altogether, these concerning developments show that there is an urgent need for a comprehensive approach to protect digital democracy. Indonesia must take firm steps to strengthen its commitment to digital rights. The government must understand the importance of a free and open internet as a foundation for democracy, and seriously work to protect its citizens from digital threats.

The 2024 General Election should be more than just a political spectacle. The election results will not just determine a new leader but will also shape the narrative of the future of digital democracy in Indonesia. For this reason, calls for action must continue to be echoed to uphold democratic values, fight digital repression, and ensure citizens' freedom of opinion.

> "This election should be more than just a political spectacle. Not only determining a new leader, but also shaping the narrative of the future of Indonesia's digital democracy.

In order to realise these ideals, collaborative efforts from the government, civil society, and the international community are needed to overcome the various challenges posed by digital rights violations. This can only be achieved by transcending political affiliation. Advocacy efforts to realise better digital freedom must continue to be pushed by the country's new leaders.

By embracing the principles of digital rights, Indonesia will not only protect its democracy and its citizens, but will also help realise the two next two lines of the election march quoted at the beginning of these epilogue: "*Hak demokrasi Pancasila, hikmah Indonesia Merdeka*.' meaning '*The democratic rights of the Pancasila, the wisdom of an independent Indonesia*'.

List of terminology

3G	:	Third-generation technology. A standard defined by the International Telecommunication Union (ITU) which generally refers to the third generation of cable-less technology development.
3T regions	:	Regions which are 'tertinggal, terdepan, dan terluar' ('left behind, frontier, and outermost') in Indonesia. 'Left behind' means low development quality, where the community is less developed than other areas nationally. 'Frontier' and 'outermost' refer to the most remote geographical locations in Indonesia.
4G	:	Fourth-generation technology of cellular telephone communication, and a development from 2G and 3G.
Accessing account without consent	:	Taking control, accessing, using, manipulating, and/or disseminating someone else's account without their permission.
ANBK	:	Asesmen Nasional Berbasis Komputer, or Computer Based National Assessment. A student evaluation program from the Ministry of Education and Culture intended to improve education quality by capturing the learning inputs, process, and outputs at education institutions.
Antivirus	:	Software used to detect and remove malware.
Authentication	:	The process of verifying the identity of someone and something. Authentication is used to prevent illegal access to a system or data, and can be done through SMS, an authenticator application, or backup codes.
BAKTI	:	Badan Aksesibilitas Telekomunikasi Indonesia Kominfo, or Ministry of Communication and Information's Indonesian Telecommunications Accessibility Agency. It has the responsibility to provide telecommunications infrastructure services funded by Universal Service Obligation Telecommunications Providers.

Biometric authentication	:	Process of verifying a person's identity based on their physical characteristics, such as fingerprints, retinas, and faces.
Breach forum	:	Dark web forums used to undertake illegal activities anonymously.
Bribe	:	Something given for services of benefits obtained.
BTS	:	Base Transceiver Station. Telecommunications infrastructure which facilitates cable-less communications between communications device and network operators. The function of BTS is to send and receive radio signals to communications devices such as mobile phones, house phones, and other devices, after which radio signals are transformed into digital signals and send to other terminals to become messages or data.
Chatbot	:	Computer programs or artificial intelligence with can be used to simulate a human-like conversation.
Complainant	:	Someone who makes a report, or provides information or a statement to law enforcement regarding a crime which will occur, is occurring, or has occurred.
Content	:	Information made available through electronic media or products. This information may consist of a variety of formats, including photographs, videos, captions on photographs and/or videos, hashtags, or metadata labels on social media, posts, geotags/ locations, reposts/retweets, live streams, and other formats.
Criminalisation	:	The determination that an activity, which was previously not considered a crime, is an act which can be punished.
Cyber gender-based violence	:	A term used by Komnas Perempuan and understood as a threat and/or sexual violence using technology and based on certain networks.
Cyber harassment	:	Digital sexual harassment through messages and comments which attack and harass, providing attention and directly contacting a person.

Cyberflashing	:	Direct distribution of intimate content without consent.
Dark web	:	A layer of the internet which consists of information that is highly secret in nature.
Data breach	:	Incidents of data leaks to parties without authority.
Data centre	:	A large group of networked computer servers which is commonly used by organisations to store remote data, perform processing, or distribute large amounts of data.
Data loss	:	The loss of data, both intentional and unintentional.
DDoS attack	:	Distributed denial-of-service attack. An attack which uses a large number of devices to flood a target with network traffic, so that the target is prevented from providing services to actual users.
Defamation	:	Acts of criminalisation with a claim for ruining one's good name.
Digital authoritarianism	:	Authoritarian regime control over a community, using technology as a form of control and observation.
Digital transformation	:	Processes and strategies using digital technology to drastically change the way a business operates and provides services.
Doxing	:	Dissemination of personal data to social media without consent. In the context of online gender-based violence, this dissemination is perpetrated by sharing a victim's personal data to be misused in 'immoral' content.
Electoral technology	:	Use of information and communication technology (ICT) in a general election, e.g. information systems related to voter data, election participant data, and election processes (such as e-voting).
Electronic sexual violence	:	The Sexual Violence Offences Law (UU TPKS) does not provide a definitive definition, but acts of electronic sexual violence can be performed through acts which record sexual content (including screenshots), disseminate electronic documents which contain non-consensual sexual content, and digital stalking.

Encrypted	:	Data which has changed format so it cannot be read without a password/code.
Encryption	:	Process of changing the format of data so it cannot be read without a password/code.
Encryption key	:	Code used to encrypt and decrypt data.
Firewall	:	Software used to block illegal access to a network.
Flaming	:	Personal attacks through personal methods. This can take place through posting attacking and intimidating comments on someone's account.
FPL	:	Forum Pengada Layanan, or Service Providers Forum. This institution was initiated by Komnas Perempuan (National Women's Commission on Violence against Women) to bring together CSOs and Komnas Perempuan's units in managing cases of violence against women. SAFEnet is part of FPL.
Freedom of expression	:	The right of every person to find, receive and disseminate information and content in any form through any means. This includes verbal expressions, published materials, and audio-visual materials, as well as cultural, artistic, and political expressions.
Hacker	:	Someone with the technical knowledge and skills to illegally access a system or data.
Hacking	:	Entering an account to steal data by using technology to obtain illegal or unpermitted access to a system or source of data, with the intention of obtaining personal information or changing/ modifying information. In online gender-based violence, hacking occurs to slander and put down a victim by using illegal access and changing their account to have a sexual nature.
IBA	:	Image-based sexual abuse. A threat to disseminate intimate content without consent by misusing intimate content as the basis for threats and exploitation.

Impersonation	:	Creation of impersonation accounts to embarrass or slander someone. This is done by making a fake account in someone else's name to disseminate false information and destroy the reputation of the person they are impersonating, including their personal life and their work life.
Information disruption	:	An umbrella term which attempts to bring together a variety of terms including: incorrect/inaccurate/ misleading news and information, fake news, hoaxes, and others. In general, this can be divided into three categories: misinformation, disinformation, and malinformation.
Information system	:	A combination of interrelated hardware, software, and telecommunication networks that people build and use to collect, create, and distribute useful data, usually within an organisational environment.
Internet disruption	:	Disruptions to internet connectivity and access. Often interchanged with 'internet shutdown', 'internet outage', and other terms.
Internet shutdown	:	Intentional disruption to the internet or electronic communications, by making said services inaccessible or effectively unusable, for a certain segment of the population or in a certain location, often to control the flow of information.
Intimate content	:	Content of an immoral, pornographic, and/or sexual nature. In Law no. 44/2008, pornographic content is understood as images, sketches, illustrations, photographs, writing, audio, sounds, moving images, animations, cartoons, conversations, bodily movements, or other forms of messages through an array of forms of communication media and/ or performances in public, which contains sexual intercourse or exploitation which violates the norms of morality in the community.
ISP	:	Internet Service Provider. Services provided by a certain company to supply internet access to the public through a subscription service.
Latency	:	Time needed to move data from one point in the network to another point.

LEO	:	Low Earth Orbit. An orbit that is relatively close to the earth, usually at an altitude of between 1,000km and 2,000km above sea level at a period of 128 minutes or less, making at least 11.25 orbits per day. Related to satellites at such an orbit, referred to as LEO satellites.
Malware	:	Software developed to destroy a system or data.
Malware analysis	:	Process of investigating malware to identify how it works and how to remove it.
Mbps	:	Megabits per second, while MBps stands for megabytes per second. The difference is in the small 'b' or capitalised 'B'. One byte is equal to eight bits.
Merger	:	The joining of two or more companies to become one company, with the lead company acquiring all assets and responsibilities of the one(s) being merged with it.
Morphing	:	Content that is manipulated to become content of a sexual or immoral nature. This is perpetrated through making a false/synthetic/created sexual image by placing an individual's face on the body of sexually performing sexual activity.
NCII	:	Non-consensual intimate image, or the dissemination of intimate content without permission. This act involves the online distribution of photographs or videos which are sexual in nature without the permission of the individual in the content, or the distribution of intimate images without consent.
Netizen	:	Someone who actively uses the internet.
Offline	:	Interactions that occur in the 'real' world (i.e. not on the internet).
Online	:	Interactions that occur online.
Online gender-based violence	:	Gender-based violence that is facilitated by technology. The violence takes the form of violence with the intention or aim of harassing a victim based on their gender or sexuality, through digital content and which influences their online life.

Online outing	:	When someone's sexual orientation and/or gender identity is shared online without their permission and with the aim of embarrassing them.
Online recruitment	:	Acts using technology which lure potential victims into certain situations which end in violence.
Online surveillance	:	Acts of monitoring, tracing, or observing someone's activities using digital technology, both online and offline.
Person reported	:	Someone who is reported to the police for committing or being believed to have committed a criminal offence, but is not necessarily the perpetrator of a criminal offence.
Personal data	:	Based on the Personal Data Protection Law, personal data is data about an individual who is identified or can be identified by itself or in combination with other data, both directly and indirectly, through electronic or non-electronic systems.
Phishing	:	Efforts to trick someone into provide personal information or money.
Platform	:	Digital space which provides facilities for users to collaborate, interact, or perform transactions.
Power relations	:	The relationship between one group and other groups based on the level of power.
Remote education	:	The process of teaching and learning conducted remotely through the use of communications media. Remote education is implemented using an array of ICT and uses learning materials which are also ICT based.
Right to be forgotten	:	The right to delete data or information that refers to characteristics, identity, and anything else about an individual, including in processes of collecting, using, or disclosing personal data.
Risk assessment	:	Process to identify and evaluate security risks.

SATRIA-1	:	Indonesia's first internet satellite, developed to meet the internet needs in frontier, underdeveloped and outermost areas ('3T').
Sextortion	:	Sexual extortion perpetrated by abusing a victim's sexual content. The perpetrator blackmails the victim by demanding financial transactions or forces them to meet for sexual activity.
Sexual violence offences	:	In Law no. 12/2022, sexual violence offences are all acts which fulfil the elements of criminal acts as regulated by the Law and other sexually violent acts as regulated by the Law to the extent specified in this Law.
SMPCS	:	Sulawesi Maluku Papua Cable System. A 8,772km-long underwater communications cable which stretches across Sulawesi, Maluku and Papua.
Social engineering	:	A technique for tricking someone into performing an undesirable action.
TF-VAW	:	Technology-Facilitated Violence Against Women. The Association for Progressive Communication (APC) states that TF-VAW refers to violence against women which is perpetrated, supported, or exacerbated, partly or wholly, using information and communication technology (ICT), such as mobile phones, the internet, social media platforms, and email.
Trusted flagger	:	Organisations and/or individuals who are trusted to identify, flag, and report illegal content. Often refers to third party partners of digital platforms.
Trusted partners	:	Parties who are recognised and trusted by digital platforms to identify, flag, and report illegal and problematic content.
Type A report	:	A complaint made by a police officer who experiences, is aware of, or directly found about the occurrence of an incident.
Undersea cable	:	Also referred to as submarine cable. An example of a backbone communication technology, laid under the ocean, to connect networks between islands and nations.

Victim of criminalisation	:	Someone who is reported as a result of their legal expression or activity on the internet, using problematic articles and regulations.
Video call (VCS/video call sex)	:	Telephone call with image, video and voice which is transmitted by one person to another person and involves sexual activity during the call.
Whistleblower	:	Someone who knows and reports certain criminal activity (or certain incidents) and is not part of the perpetrators nor the victims (as per definition by the Indonesian Supreme Court).
Zero-day exploit	:	Security vulnerabilities that are not known to software vendors.

References

Part 1: Internet Access

1 Nic Cheeseman, Gabrielle Lynch & Justin Willis (2018) Digital dilemmas: the unintended consequences of election technology, Democratization, 25:8, 1397-1418, DOI: 10.1080/13510347.2018.1470165

2 https://www.voaindonesia.com/a/kpu-siapkan-peta-jalan-penggunaan-teknologi-untuk-pemilu-2024/6292788.html

3 https://www.suara.com/tekno/2023/11/30/112232/kominfo-pastikan-jaringan-internet-moncer-selama-pemilu-dan-pilpres-2024

4 https://m.kominfo.go.id/content/detail/53256/siaran-pers-no-512hmkominfo112023-tentang-sukseskan-pemilu-2024-menteri-budi-arie-kominfo-siapkan-infrastruktur-digital/0/siaran_pers

5 https://politik.rmol.id/read/2023/09/08/588241/ini-cara-mudah-masyarakat-laporkan-dugaan-pelanggaran-pemilu-2024

6 https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

7 https://yogyakarta.kompas.com/read/2023/12/14/114010078/susah-sinyal-nasib-rekapitulasi-pemilu-online-di-wilayah-gunungkidul-ini?page=all

8 https://lampung.antaranews.com/berita/699783/608-tps-di-bengkulu-akses-sulit-dan-tak-terjangkau-internet

9 https://www.cnbcindonesia.com/tech/20231227115647-37-500530/proyek-bts-4g-kominfo-selesai-besok-dibuktikan-di-ujung-ri

10 https://www.cnbcindonesia.com/research/20231227154444-128-500631/daftar-lengkap-bts-4g-kominfo-ujung-aceh-ke-pedalaman-papua

11 https://www.cnbcindonesia.com/tech/20231227204834-37-500756/akan-diresmikan-jokowi-bts-bakti-bukti-pemerataan-digital-ri

12 https://papua.tribunnews.com/2024/01/04/jaringan-telekomunikasi-di-merauke-kambali-putus-ini-penyebabnya

13 https://kids.republika.co.id/posts/257348/berapa-jumlah-sekolah-di-indonesia-dari-tk-sampai-sma

14 https://www.infopublik.id/kategori/nusantara/790257/jaringan-internet-lemot-siswa-

di-kusu-sinopa-gelar-anbk-di-pinggir-pantai

15 https://katanetizen.kompas.com/read/2023/11/12/204518585/sulitnya-internet-untuk-anbk-sekolah-pelosok-butuh-sarana-memadai?page=all

16 https://www.detik.com/jatim/berita/d-7010744/puluhan-siswa-trenggalek-jalani-anbk-di-tengah-hutan-pinus-ini-penyebabnya

17 https://www.mediapromed.com/news/100310465509/kominfo-putus-jaringan-internet-di-baduy-dalam-desa-kanekes-resmi-jadi-kawasan-blank-spot-internet

18 https://teknologi.bisnis.com/read/20231019/101/1706054/bukan-ingin-membandingkan-internet-indonesia-memang-makin-lemot-kuartal-iii2023

19 https://www.cnnindonesia.com/teknologi/20231027142013-192-1016721/kelakar-menkominfo-soal-internet-ri-masih-lemot-kayak-ranking-fifa

20 https://www.detik.com/sulsel/berita/d-6904052/memprihatinkan-kecepatan-internet-indonesia-nyaris-paling-rendah-se-asean

21 https://goodstats.id/article/internet-banyak-digunakan-perusahaan-penyedia-internet-di-indonesia-makin-bertambah-oad9v

22 https://teknologi.bisnis.com/read/20230920/101/1696996/jumlah-isp-melesat-pada-2022-terbanyak-dalam-6-tahun-terakhir

23 https://teknologi.bisnis.com/read/20230921/101/1697342/starlink-muncul-apjii-pede-jumlah-isp-lokal-baru-tetap-melesat

24 https://www.cnbcindonesia.com/tech/20230829142629-37-467126/beda-kecepatan-internet-ri-dengan-starlink-elon-musk-simak

25 https://finance.detik.com/infrastruktur/d-7123174/starlink-elon-mau-masuk-ri-menkominfo-pilih-pakai-satria-1

26 https://www.sugawa.id/nasional/10048946045/kisah-pilu-warga-ntt-korban-janji-manis-johnny-g-plate-sinyal-lemot-susah-dipakai-menelepon

27 https://samudrafakta.com/menara-bts-bakti-berdiri-sinyal-malah-hilang/

28 https://regional.kompas.com/read/2023/05/26/121923678/cerita-warga-di-sumbawa-naik-gunung-cari-sinyal-internet-bts-dari-desa-lain?page=all

29 https://lampung.antaranews.com/berita/685755/tower-bts-berdiri-jaringan-internet-di-desa-3t-wayharu-tetap-lemot

30 https://kaltara.tribunnews.com/2023/05/23/warga-desa-seputuk-keluhkan-jaringan-internet-lemot-berharap-solusi-dari-diskominfo-tana-tidung

31 https://www.odiyaiwuu.com/2023/05/08/ravenirara-kabupaten-informasi/

32 https://www.sairerinews.com/2023/05/06/warga-ansus-keluhkan-jaringan-internet-pengguna-android-meningkat/

33 https://www.cnbcindonesia.com/tech/20231228191515-37-501090/internet-di-pedalaman-masih-lelet-ini-kata-bos-bakti-kominfo

34 https://www.kompas.id/baca/riset/2023/06/29/menyoal-harga-dan-gangguan-layanan-internet-seluler-di-indonesia

35 https://www.viva.co.id/berita/bisnis/1640888-warganet-heboh-m-banking-bca-eror-dan-saldo-di-atm-nol-rupiah-manajemen-buka-suara

36 https://www.viva.co.id/digital/digilife/1599985-lockbit-3-0-diduga-bobol-data-nasabah-bank-syariah-indonesia

37 https://selular.id/2023/10/kominfo-dorong-hanya-3-operator-seluler-di-indonesia-simak-tanggapan-atsi/

38 https://www.liputan6.com/surabaya/read/5428601/kominfo-klaim-putus-akses-425-ribu-konten-judi-online-hingga-oktober-2023-gandeng-sejumlah-provider-internet

39 https://aptika.kominfo.go.id/2022/09/mekanisme-pemblokiran-konten-negatif/

40 https://tekno.kompas.com/read/2023/09/22/09202577/kominfo-sudah-pulihkan-google-docs-bukan-diblokir-tapi-kesalahan-teknis

Part 2: Freedom of Expression

41 https://freedomhouse.org/country/indonesia/freedom-net/2023

42 https://floresa.co/mendalam/56455/2023/09/19/bupati-manggarai-barat-jerat-warga-dengan-uu-ite-pegiat-ham-korban-ketidakadilan-tak-layak-dipidana

43 https://www.viva.co.id/trending/1568535-serang-balik-eks-karyawan-jhon-lbf-dia-mohon-mohon-sampai-nangis-minta-kerjaan

44 https://www.tribunnews.com/seleb/2023/04/15/laporkan-pengacara-ae-john-lbf-tegas-tidak-akan-ambil-jalur-damai

45 https://www.cnnindonesia.com/nasional/20231208162516-12-1034776/aktivis-karimunjawa-daniel-frits-ditetapkan-tersangka-sejak-mei-2023

46 https://www.gatra.com/news-567497-hukum-aspri-wamenkumham-polisikan-ketua-ipw-sugeng-teguh-santoso.html

47 https://www.beritasatu.com/nusantara/1072580/keluarga-ronald-tannur-laporkan-balik-kuasa-hukum-dan-keluarga-korban

48 https://news.detik.com/berita/d-6782163/akun-penyebar-video-bobby-beda-sikap-

ke-bendera-pdip-golkar-dipolisikan

49 https://www.detik.com/jateng/berita/d-7113279/pdip-solo-ngadu-ke-polisi-soal-video-simpatisan-deklarasi-dukung-paslon-02

50 https://www.liputan6.com/regional/read/5489155/anies-baswedan-dilaporkan-ke-bareskrim-soal-akronim-amin-jubir-timnas-amin-cari-sensas

Part 3: Digital Security

51 https://twitter.com/neohistoria_id/status/1695817893651636439

52 https://www.tribunnews.com/nasional/2023/05/08/pasukan-08-prabowo-klaim-mampu-lacak-nama-dan-alamat-pelaku-ujaran-kebencian-di-jagad-maya.

53 https://nasional.tempo.co/read/1786733/instagram-bem-universitas-udayana-diretas-usai-kritik-dinasti-politik-jokowibem-lain-pernah-mengalami

54 https://surabaya.kompas.com/read/2023/12/06/174733578/merasa-diintimidasi-butet-aku-kehilangan-kemerdekaan

55 https://www.cnbcindonesia.com/tech/20231129072836-37-492847/204-juta-data-pemilih-bocor-dibobol-hacker-kpu-buka-suara

56 https://www.cnnindonesia.com/nasional/20230805193203-20-982398/situs-bawaslu-makassar-dua-kali-diretas-berubah-jadi-judi-online

57 Andreas Takimai, dkk., "Installah Aku, Kau Kuma-matai", SAFEnet, Oktober 2023

58 Benediktus Fatubun, "Jurnalis The Papua Journal Dilarang dan Digeledah Saat Akan Liput Sidang Victor Yeimo", thepapuajournal.com, 31 Januari 2023, https://www.thepapuajournal.com/tahan-papua/pr-6987200771/jurnalis-the-papua-journal-dilarang-dan-digeledah-saat-akan-liput-sidang-victor-yeimo?page=1

59 https://tekno.kompas.com/read/2023/08/10/12150037/ponsel-kapolda-jateng-diretas-via-file-apk-penipuan-ini-ciri-ciri-modusnya

Part 4: Online Gender-based Violence

60 Tribunnews.com "*Viral Video 21 Detik Bacaleg Nasdem Telanjang, Kini Mengundurkan Diri Usai Rekaman Tersebar*". Article can be accessed at https://www.tribunnewswiki.com/2023/08/23/viral-video-21-detik-bacaleg-nasdem-telanjang-kini-mengundurkan-diri-usai-rekaman-tersebar

61 Tribunnews.com "Siswa SMA NTT Gantung Diri Usai Foto Bugil Viral, Polisi Ungkap Kronologi dan Calon Tersangka". Article can be accessed at https://sulbar.tribunnews.com/2023/10/03/siswi-sma-ntt-gantung-diri-usai-foto-bugil-viral-polisi-ungkap-kronologi-dan-calon-tersangka

62 Salabi, Nurul Amalia. Presentation of Association for Election and Democracy (Perludem) “Beware of Digital Attacks Ahead of the 2024 Election” during closed discussion hosted by SAFEnet, July 2023.

63 Number of OGBV cases in three institutions over the last 3 years. Source (LBH APIK, 2021, 2022, & 2023; Komnas Perempuan, and SAFEnet, 2023. The number of OGBV from Komnas Perempuan 2023 was obtained from the Service Provider Unit of Komnas Perempuan referrals to SAFEnet via the SAFEnet Hotline.

64 Kbri.id “Kasus Eksploitasi seksual pada Anak Melalui Internet Meningkat pada 2023”. Article can be accessed at di https://kbr.id/nasional/12-2023/kasus-eksploitasi-seksual-pada-anak-melalui-internet-meningkat-di-2023/113814.html

65 A blog site uploads intimate VCS content with several male victims. VCS content is a manipulation where the perpetrator creates a narrative that he is a victim of extortion, the victim is recorded with his face visible, accompanied by captions with victim information, proof of payment (before being threatened), and even social media information.

66 Data taken based on SAFEnet processing in Quarter 4 (October – December) 2023. Detailed information is confidential. This data is also adjusted based on availability questions to be published on the form at aduan.safenet.or.id.

67 Ibid

68 “Their hopes regarding digital rights are more related to economic and infrastructure issues. This differs from participation from the general group, whose expectations are mostly related to issues of freedom of expression and digital security.” For more information, see Amabel, Winona and Surya Putra B. Being Queer on the Internet: Restrictions on Expression and Digital Attacks on Individuals and Groups with Diverse Genders and Sexualities in Indonesia. Jakarta: Remotivi, 2023, p. 24

69 Amabel, Winona and Surya Putra B. Being Queer on the Internet: Restrictions on Digital Expression and Attacks on Individuals and Groups with Diverse Genders and Sexualities in Indonesia, Jakarta: Remotivi, 2023, p. 34

70 The post circulated on Twitter @PunkIsD**, who claimed to be a health worker at one of the government health services in West Java. He published a photo secretly and wrote a tweet with the narrative, “Just finished (the HIV test), another high school student came. “No wonder HIV cases in the district are increasing,”. This post has been taken down by Twitter.

71 One of the accounts that outed the organizers of Queer Advocacy Week was the @ assi**** account on one of the social media. The account describes several individuals who were organizers of the event with the narrative “LGBT groups and LGBT advocacy activists”.

72 Some media outlets have taken a role in building this bad image. See more in the press release at https://aji.or.id/read/press-release/1600/media-massa-diskriminatif-beritakan-asean-queer-advocacy-week.html

73 Sidoarjo District Court Decision Number ***/Pid.B/2023/PN.Sda on 11 September 2023. The defendant was an office boy who secretly recorded the victim in the toilet of an office. The verdict is kept secret. Source https://bangunan3.mahkamahagung.go.id/direktori

74 Creepshot is the act of secretly taking photos or recording other people's objects for sexual purposes. More details can be seen at Rachmawati, Maidina, and Nabillah Saputri. Jauh Panggang dari Api : Menilik Kerangka Hukum Kekerasan Berbasis Gender di Indonesia. Bali : Southeast Asia Freedom of Expression Network, 2022, p. 22. Book can be accessed at https://awaskbgo.id/kerangkahukum/

75 Yofira, Alia., Ellen Kusuma., Justitia Avila Veda., Maidina Rachmawati., Muhammad Daerobi. Policy Paper: The Urgency of Arranging the Removal of Electronic-Based Sexual Violence Content in Favor of Victims. Published on SAFEnet on https://safenet.or.id/id/2023/05/kertas-kebijakan-mengenai-urgensi-pengaturan-penghapusan-konten-kekerasan-seksual-berbasis-elektronik-yang-berpihak-pada-pemenuhan-hak-korban/

76 https://freedomhouse.org/report/election-watch-digital-age#indonesia-2024