Joint stakeholder contribution
Freedom of expression, freedom of religion and belief, and digital rights
1.1. In this submission, the Association of Progressive Communications (APC), EngageMedia and Southeast Asia Freedom of Expression Network (SAFEnet) examine Indonesia’s compliance with the recommendations received during the third Universal Periodic Review cycle in 2017. This submission will focus particularly on digital rights including freedom of expression, the protection of human rights defenders (HRDs), including women human rights defenders, violence against women and misinformation.

1.2. APC, an organisation in consultative status with ECOSOC, advocates the strategic use of information and communications technologies to advance human rights. The APC network has 62 organisational members and 29 individual members active in 74 countries.

1.3. EngageMedia is a nonprofit that promotes digital rights, open and secure technology and social issue documentary. Combining video, technology, knowledge and networks, EngageMedia supports Asia-Pacific and global changemakers advocating for human rights, democracy and the environment. In collaboration with diverse networks and communities, EngageMedia defends and advances digital rights.

1.4. SAFEnet is a regional digital rights organisation based in Denpasar, Indonesia. SAFEnet was founded with a vision of realisation of a digital space that upholds human rights values for all people. Its mission is to defend digital rights in the Southeast Asia region, including the right to access the internet, the right to express freely and the right to feel safe in digital spaces. SAFEnet has been actively advocating for victims of digital rights violations, especially critical groups who use the internet as a tool for expression and opinion.
2.1. During the third UPR cycle, Indonesia received 28 recommendations on the rights to freedom of expression and freedom of religion and belief. Of the 28 recommendations received, only 20 were accepted, and eight were noted.

2.2. Tracing back to the previous UPR cycle up until this date, the Indonesian government is partially implementing the recommendation to combat discrimination and violence against women based on numbers 139.27, 139.28 and 139.119. The legal framework for combating violence against women and children is still in the drafting process (RUU TPKS) and has not been passed yet.¹

2.3. The government is partially implementing recommendation numbers 139.73, 141.42, 141.26, 141.28 and 141.57 to ensure and revise national and regional laws that do not discriminate or limit certain group’s rights based on their religion and belief.²

2.4. The government does not comply with the recommendations number 141.27 and 141.34 on repealing or eliminating the blasphemy law. Even more, the new Criminal Code Draft contained several articles relating to blasphemy.³

2.5. The government can be considered unwilling to comply with 139.64 and 139.66 on protecting HRDs. Other than The National Commission on Human Rights (Komnas HAM), regulation on human rights protection procedures that have been violated often and still criminalise HRDs. Indonesia has not shown its commitment to protecting HRDs, especially those who express their voices in digital spaces.⁴ ⁵

2.6. Regarding online freedom of expression, the protection for freedom of expression in international law is based under Article 19 of the Universal Declaration of Human Rights (UDHR) and under Article 19 of the International Covenant on Civil and Political Rights (ICCPR). Both protect the right to freedom of expression of individuals, including their right to seek, receive and impart information through the media, including online.

2.7. In Indonesia, this protection is based under Law No. 39/1999 (Article 23(1) and 25) and the Indonesian Constitution (Article 28E). Both stipulate that every person shall be free to express his or her opinions in public. Article 28E(3) of the Indonesian Constitution also protects the rights to seek, receive and impart information and ideas, orally and in writing, through printed and electronic media.

². 2006 Joint Regulation of the Minister of Religious Affairs and the Minister of Home Affairs No. 8 and 9/2006, 2008 Joint Decree of the Minister of Religious Affairs, the Attorney General and the Minister of Home Affairs, Law No. 11 of 2020 on Job Creation.
³. Article 304-308 Indonesia’s Draft Criminal Code 2019, Article 156 and 156(a) of the Criminal Code and the 1965 Presidential Decree (No. 1/PNPS/1965)
2.8. However, based on SAFEnet’s digital rights situation reports from 2018 through 2021, there are 56 cases targeted toward journalists, activists, HRDs and academicians being prosecuted using Article 27 paragraph 3 and article 28 paragraph 2 of the Information Electronic Transactions (ITE Law).  

2.9. The UN Human Rights Council Resolution in 2012 also recognises the global and open nature of the internet as a driving force in accelerating progress towards development in its various forms; and calls upon all states to promote and facilitate access to the internet and international cooperation aimed at the development of media and information and communications facilities in all countries. This resolution compels every country to provide protection for freedom of expression in the online world and guarantees equitable and fair internet access.  

2.10. However, based on SAFEnet reports from 2019 through 2021, the Indonesian government has shut down the internet in Papua and West Papua. In 2019, the Indonesian government slowed down the internet from 19 to 21 August 2019, followed by the internet shutdown from 22 August to 4 September 2019. Then in 2020, there were four reports alleging bandwidth throttling (partial shutdowns). In 2021, there were another 12 internet outages, where eight internet shutdowns were allegedly related to Indonesian military operations.  

2.11. The internet can encourage the promotion and advocacy of human rights. The presence of the internet is used by HRDs to expand their work and to campaign for the protection of human rights. As such, HRDs play an important role in monitoring violations as well as advancing the condition of human rights globally.  

2.12. The 1998 UNGA Declaration on Human Rights Defenders recognises the importance and legitimacy of the work of HRDs, as well as their need for better protection. The recent UNGA resolutions on HRDs, among other things, call upon states to take “appropriate measures for the prevention of all forms of violence, intimidation, threats and attacks against human rights defenders on the internet and through digital technologies, and to protect human rights defenders, including women human rights defenders, in online spaces and to consider adopting laws, policies and practices that protect them from defamation and hate speech while also affirming the rights to freedom of expression and privacy” and “to refrain from the use of surveillance technologies against human rights defenders”.  

2.13. The adoption of the Declaration on Human Rights Defenders has given recognition to HRDs and increased their visibility, while paving the way for the establishment of a UN mechanism for their protection. Not only does it guarantee the rights of HRDs, this declaration also emphasises the duty and role of the state to protect, promote and implement human rights and ensure that everyone under national law can enjoy all these rights, as stated in Article 2.

---

2.14. Komnas HAM said that between 2020 and 2021, most cases of violations of freedom of expression occurred in the digital space. In five recent years, digital attacks against HRDs in Indonesia have tended to increase. Based on SAFEnet monitoring, for instance, at least 193 incidents of digital attacks took place in 2021. This is an increase of 38% compared to the previous year in 2020, which saw 147 incidents.¹⁰

2.15. Indonesia has also ratified the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). However with the absence of regulations that are pro-survivors of sexual violence alongside the impact of the COVID-19 pandemic, sexual gender-based violence has increased in Indonesia, with a four-fold increase in online gender-based violence (OGBV) cases or 510 cases.¹¹¹²¹³

2.16. To date, there are some regulations and new laws that curb freedom of expression, freedom of religion and belief, and digital rights in Indonesia, such as:

- Presidential Decree Number 1/PNPS/1965 Concerning The Prevention of Religious Abuse and/or Defamation.
- Articles 156 and 292 of the Criminal Code.
- Article 27(3), 28(2) ITE Law 2008.
- Article 4 and 8 Law No. No 44 of 2008 on Pornography Law.
- Article 27(1), 29 and 36 Joint Regulation of the Minister of Communication and Information Technology, Attorney General and National Police Chief No. 229 and 154 year 2021 on guidelines on implementing ITE Law.
- Article 9, 13, 15 and 16 Ministerial Regulation Number 5 year 2020 on Private Electronic System Provision.
- Indonesian Police Telegram Letter No. ST / 1100 / IV / HUK.7.1\ \ / 2020; contains instructions regarding legal action towards the "spreaders of false information" and all actions against the President and his government on handling the COVID-19 pandemic in digital spaces.¹⁴
- Indonesian Police Telegram Letter No. STR/645/X/PAM.3.2./2020; This authorises the police on handling the mass protest in public space also to conduct a "cyber patrol" for every "objection content" on Government works (especially the legalisation of the Omnibus Law) in digital spaces.¹⁵
- Article 6 Communications and Informatics Ministerial Regulation No. 12 of 2016 on prepaid SIM card registration.

¹² SAFEnet research: http://awaskbgo.id/kerangkahukum
SECTION 3: ONLINE VIOLENCE AGAINST WOMEN

3.1. Violence against women is a human rights violation and universal issue with severe impact on victims/survivors, their families and communities. As the COVID-19 pandemic deepens economic and social stress coupled with restricted movement and social isolation measures, gender-based violence is increasing exponentially.16

3.2. During COVID-19, violence against women, in the forms of domestic violence and online and ICT-facilitated violence or online gender-based violence (OGBV), spiked in situations where no regulations were capable of resolving OGBV, especially with regards to providing protection to victims.

3.3. In 2018, the National Commission Against Women Violence (Komnas Perempuan) documented 97 cases of OGBV. In 2019, the number increased to 281 cases, and in 2020, a total of 940 OGBV cases were recorded. The same trend was found in reports from OGBV service providers to Komnas Perempuan, which reported 126 OGBV cases in 2019 and 510 OGBV cases in 2020.

3.4. The victims face many challenges, one of which is the fear of prosecution under laws like the Electronic Transactions and Information Law (UU ITE) and the Pornography Law (UU Pornografi). This is especially the case if the victim was involved in the creation of digital intimate content.

3.5. Other challenges included difficulties in obtaining evidence, jurisdictional issues that are different to conventional criminal acts, limited scholars or academicians with understanding of OGBV, limited availability of digital forensic technology, technical elements of trials, and the continuing poor perspective of law enforcement officials on OGBV.

3.6. Another challenge is the prosecution of the victim of non-consensual content distribution.17 The OONI 2021 report also mentions LGBTIQ-related internet censorship found in Indonesian online communities, where LGBTIQ persons were censored together with international queer news sites and queer dating apps.18

---


Recommendations:

- The state revokes regulations that are discriminatory, were not developed based on human rights principles and have a disproportionate impact on women and gender minorities, especially Article 27 clause (1) of UU ITE, which needs to be designed in line with the concept of "consent" based on principles of the right to bodily authority. It is also recommended that all provisions in the Pornography Law be improved to ensure that pornography is prohibited not based on protecting social morality norms but on principles of the right to bodily integrity and personal data.

- The state must develop a regulation for case management and protection specific to OGBV victims, including among others, a provision of rights to individuals to request the removal of information and personal data from the internet. Alongside this regulation, a system in which OGBV victims can request the imposition of sanctions or interventions against perpetrators who distribute content without consent as well as service providers who carry said content should also be developed. Also a provision for counselling services as well as search features and contact details on platforms, websites and blogs should be created in order to erase and remove image-based content reported by victims. Lastly, a provision for a public information system about service providers’ compliance with measures to prevent and handle OGBV should also be developed.

- The Human Rights Commission resolution from 2018 on preventing and responding to violence against women and girls in digital contexts recommends that states:
  - Ensure that legislation allows for the timely and effective investigation, prosecution, sanction and redress of violence against women and girls in digital contexts.
  - Encourage business enterprises in the effective implementation of the Guiding Principles on Business and Human Rights to protect the private data of women and girls, to create transparent and effective processes for reporting violence and to develop policies that meaningfully protect women and girls from violence in digital contexts.¹⁹

- The state must build public awareness on OGBV in the education sector for the public, young people and law enforcement officials.

- The state needs to lift all forms of censorship and suppression of information on the internet.

- The state shall prevent, prosecute and punish all forms of OGBV including sexual harassment, stalking and non-consensual dissemination of intimate images.

---

SECTION 4: PROTECTION FOR HUMAN RIGHTS DEFENDERS

4.1. The Indonesian state, both at the central and local levels, has a long history of outsourcing privatised violence to maintain and strengthen the political and economic interests of state actors. These privatised violence actors harass and intimidate. These include attacks and persecution by moral vigilantes such as Islam Defender Front (FPI) and other private initiatives, conducted both online (cyberbullying and trolling, “outing” gender minorities and hate speech) and offline through intimidation, harassment, stalking and physical violence.20

4.2. This practice continues and has even amplified since 2017 as it reached digital spaces through the deployment of “political buzzers” (cyber troops) as political trolls harassing dissenters, especially targeted to human rights defenders.21

4.3. The harassment and intimidation is also targeted toward WHRDs. The online space opens the door to new forms of violence such as online harassment, doxxing, sending sexually explicit content and threats of rape. The types of OGBV targeting WHRDs found include breaches of privacy, surveillance and monitoring, damage to reputation/credibility, harassment and threats to violence, direct threats and violence, and attacks targeted at certain community. The OGBV that most often occurs are hate comments that have not attacked gender identity, trolling in the form of sexually suggestive and degrading expressions, including intentionally sending intimate photos without being asked, and photo manipulation either to demean (e.g. memes) or sexually nuanced (e.g. to make pornographic content). Other OGBV come in the form of hate speech, namely calls and invitations to take physical violence against the victim (beating, murder, rape) and threats of violence directed at the victim or her family, as well as threats of rape or death threats.22

4.4. In 2021, the establishment of “virtual police” further risked the privacy of HRDs. This “virtual police” force was established with a circular letter numbered SE/2/11/2021 concerning Awareness of Ethical Culture to Create Clean, Healthy, and Productive Indonesian Digital Space. The implementation of “virtual police” only aimed to remove critical content published in social media.

4.5. Since “virtual police” was first established, at least 476 accounts have received a warning for allegedly containing hate speech content. However, the measure of hate speech has never been precise. The increase in numbers shows that the implementation of the “virtual police” has become a new tool of repression in the digital world, as they threatened the public’s freedom of expression on social media.23

---

4.6. Regarding online privacy, apparently the state has made no serious efforts in guaranteeing data security, both digitally (digital infrastructure) and physically (security measures in building). The major power outage in Jakarta in 2019 and the fire at Cyber 1 Datacenter building in 2021 crippled many urban activities through which HRDs operate. Also frequent personal data leaks (numbers, addresses, photos, etc.) occur from both government and private companies’ databases. This leaked user data is usually sold on the black market or even in certain corners of online marketplaces. Leaked data can be used to harass dissenters.24

4.7. Under Ministry of Communication and Information Technology Regulation Number 5 year 2020, the private companies (Electronic System Operators) are required to provide user data to the government when asked. This data can include biometrics, health, genetics, sexual orientation, political views and financial records. This may pose a privacy risk for HRDs.25

**Recommendations:**

- The state needs to ensure privacy protection and transparency in their collection and use of data. There is a need to push forward Laws on Data Protection. The state also needs to designate data centres as a vital state object with proper infrastructure on both digital and physical security.
- The state needs to stop politicising the label “hoax” and “radicalism” to deter dissent. Crackdown on “radicals” could further alienate and polarise religious communities which cause more damage to HRDs.
- The state needs to fully enforce existing protection for HRDs, making comprehensive, holistic and integrated protective regulations and policies for HRDs, especially from OGBV faced by WHRDs.

---

SECTION 5: DISCRIMINATION AGAINST MINORITY GROUPS

5.1. Indonesia ratifies CEDAW to eliminate all forms of discrimination against women and gender minorities. However under Article 27 paragraph 1 of ITE Law, any person in Indonesia is prohibited from “distributing, transmitting, and producing of any digital content that violates decency.” This article often used to prosecute minority groups. In early 2018, the Wahid Foundation released the results of its survey on intolerance among Muslim women in Indonesia. The study showed minority groups as the principal targets of intolerance. These include religious and political minorities, as well as lesbian, gay, bisexual and transgender (LGBTIQ) communities. Decency and pornography statutes cannot be separated from conservative Islamic classifications of what is proper and improper.

5.2. This phenomenon also infiltrates multiple layers of Indonesian society through “Hijrah” trends where Islamic morality and practices entered the mainstream and gained wider appeal. Such a movement also rises on social media, namely IndonesiaTanpaJIL, One Finger Community and UdahNikahinAja/IndonesiaTanpaPacaran where pop culture references are used to appeal to younger audiences.

5.3. An anti-LGBTIQ group started in higher education institutions in Indonesia.26

5.4. In 2017, the constitutional court rejected AILA (a conservative organisation started by a lecture from Bogor Agricultural Institute) judicial review to criminalise LGBTIQ communities and fornication.27

5.5. Indonesia’s Draft Criminal Code 2019 expands the list of “components of offences” for blasphemy, such as:

- Article 304-305: Criminalisation for blaspheming Indonesia’s six officially recognised religions – Islam, Protestantism, Catholicism, Hinduism, Buddhism and Confucianism (in line with the current Blasphemy Law).
- Article 306: Criminalisation towards anyone who incite others to abandon their faith.
- Article 308: Criminalisation towards anyone who insults others conducting or leading religious practices.

Recommendations:

- The state must comply with all of its obligations under CEDAW to eliminate all forms of discrimination against women and gender minorities.
- The state must affirm people of all sexual orientations and gender identities and protect their sexual and gender expression on the internet.

---


• The state shall repeal all religious/decency laws that directly and indirectly discriminate against women and LGBTIQ persons on the internet, including article 292 of Criminal Code.

• The state should stop and prevent all forms of online discrimination, harassment and abuse by law enforcement officers targeted at women and LGBTIQ persons.

• The state should fund and support women and LGBTIQ civil society organisations and community groups to provide psychosocial and legal assistance to survivors of OGBV and discrimination.

• The state should set up and reinforce formal mechanisms to include women and LGBTIQ organisations and groups in policy making, legislative and judicial processes (e.g. consultation, parliamentary hearing, amicus curiae).
6.1. Recently reported by the Indonesian Legal Aid Foundation (YLBHI), the type and number of groups charged with blasphemy laws is increasing. In 2020, 67 cases of blasphemy occurred, and 43 of these cases occurred due to the dissemination of content on social media. For example, youtuber “Muhamad Kece” was arrested by the police under blasphemy allegation of his content on kitab kuning (traditional set of the Islamic texts used by the educational curriculum of the Islamic seminary in Indonesia).28

6.2. Those prosecuted with the blasphemy law will later be charged under Article 156 and 156(a) Criminal Code, which imposes a five-year prison sentence “for whosoever in public intentionally express their views or engages in actions: a. that in principle incite hostilities and considered as abuse or defamation of a religion embraced in Indonesia.”

6.3. Law enforcement have been using “religious harmony” (kerukunan beragama) as a norm to uphold when living among people with different religious beliefs. Therefore, if anything or anyone violates the “harmony”, they can be penalised using whatever legal instrument is available.

6.4. In addition to the cases illustrated above, there are two other examples: a man was sentenced to three years in jail after tearing a Quran29 and a woman was found guilty for carrying a dog into a mosque.30 Most of the arbitrary persecution happened under a majoritarianism bias where only marginalised religious groups were under scrutiny.31 Equal treatment was absent when when the victim was part of a religious minority group. In the case of a viral video of a man throwing offerings in Mount Semeru’s eruption in 2022, there was no legal prosecution against him.32

Recommendations:

• The state needs to comply with obligations under ICCPR to respect, promote and protect the rights of all people to freedom of thought, conscience, religion and belief.
• The state needs to repeal blasphemy laws that contravene the right to profess and manifest religion or belief online.
• The state should exercise restraint in enforcing any laws that may restrict freedom of expression and freedom of religion on the internet – any restrictions that must be provided for by law should be necessary and proportionate.
• The state should strengthen the protection of minority religious groups from online hate speech and crimes.
• The state should support civil society initiatives to foster religious tolerance, acceptance and harmony amongst the Indonesian public.

7.1. In particular, since 2019, there has been a marked increase in campaigns of cyber troops working to mobilise public conventions for collaborative government policies, such as the revision of the Corruption Eradication Commission Law in September 2019, the launch of the New Normal policy during the COVID-19 pandemic in May 2020, and the ratification of the Job Creation Omnibus Law in October 2020. In all three cases, cyber troops made deals by flooding the media with narratives that pushed the government’s agenda, often resorting to deception and disinformation by multiple “buzzer” and “bot” accounts. Thus effectively drowning out oppositional discourse on social media and neutralising dissent, especially as mainstream media simultaneously echoes the cyber troop narrative.

7.2. Political and economic elites, including state actors, have mobilised “political buzzers” (computational propaganda, cyber troops, etc.) for the purpose of propaganda, political trolling and disinformation. The mobilisation is closely related to the political campaign industry.

7.3. Central government is trying to intervene in the conduct of governance in local levels in the name of maintaining “social stability”. As such, CSOs are apprehensive in arguing that disinformation damages social stability because the state has used “social stability” to justify silencing dissent, as in the case of shutting down the internet during Papua conflict in 2019.

7.4. EngageMedia Digital Rights report finds that the label “hoax” and “fake news” are “politicised”. The state has used the labels “fake news” or “hoax” to selectively put people in jail.

7.5. The state and civil society organisations have relied on digital and media literacy as a panacea to combat disinformation (including workshops), but it has been very difficult to measure the impact.
**Recommendations:**

- The state shall repeal laws that unnecessarily and disproportionately limit online freedom of expression.

- The state needs to push laws for stricter monitoring of the transparency of campaign funding for the purpose of election and government communication. This law has to include private funds from state actors and non-state actors with political connections, such as business magnates. This law is supposed to track the funding of organised disinformation/propaganda and regulation of the political campaign industry.

- The state has to require social media platforms with offices in the country to observe several obligations, such as the assembly of a team of contextual human moderators, the involvement of elements from CSOs (activists, journalists, local figures, etc.), using less automated moderation to improve fact checking and analysing of potential harm that might be caused by social media content (including disinformation), and ensure platforms are always humanely responsive to the possibility of appeal by users in cases of misattributed sanction.

- The state has to make data ethics efforts mandatory for information technology workers in the industry in order to mitigate harm caused by ignorance in developing technological systems.
SECTION 8: INTERNET SHUTDOWN IN PAPUA

8.1. The UN Human Rights Council Resolution in 2012 also recognises the global and open nature of the internet as a driving force in accelerating progress towards development in its various forms. It calls upon all states to promote and facilitate access to the internet and international cooperation aimed at the development of media and information and communications facilities in all countries. This resolution compels every country to provide protection for freedom of expression in the online world and guarantees equitable and fair internet access.39

8.2. However, based on SAFEnet reports from 2019 through 2021, the Indonesian government has shut down the internet in Papua and West Papua. In August and September 2019, internet access was shut down, but calls could still be made based on the government’s instruction due to anti-racism demonstration in numerous Papua cities.40 Later in June 2020, Jakarta District Court decided that the internet shutdown was unlawful.41

8.3. In 2020, there were cases of internet shutdowns and throttling due the heightened conflict in Nduga and Maybrat, as well as during the anniversary of the anti-racism rally in August 2020.42

8.4. From April through June 2021, there were internet interruptions in Jayapura and its subdistrict, Keerom. In Sarmi internet was only available in some areas. Officially, the interruption was due to underwater fibre optic cable damage, but the interruption also coincides with discussion around special autonomy legislation, military operation and Victor Yeimo’s arrest.43 On 25 August 2021, there was an internet interruption in Jayapura due to Jokowi’s visit on 26 August 2021.44

8.5. On 25 January 2022, the internet and GSM network were not working properly in Papua due to underwater cable system interruption in Celebes, Maluku and Papua (SMPCS), but the timeline also corresponds to horizontal conflict in Sorong.45

8.6. In February 2022, an internet outage happened in Wadas village during their resistance against quarry mining.46 47

8.7. These internet shutdowns impact the right to education and health especially during the COVID-19 pandemic. In Indonesia, where 122 districts are classified as 3T districts. Most are in three provinces: Papua, West Papua and East Nusa Tenggara. As in 2020, in 2021 schools in these three provinces continued to face difficulties with internet access when having to implement distance learning due to the pandemic. While struggling with limited internet connectivity, especially in mountainous areas, people in Papua and West Papua suffered from at least 16 incidents of internet outages between 2020 and 2021, as recorded by SAFEnet. As a result, the residents were unable to communicate via the internet. In fact, sometimes there was not even a mobile phone signal. These conditions complicated their right to education through online learning.

8.8. In Sisir Dua Village, Makbon Subdistrict, Kaimana District and West Papua, instead of conducting classes online, teachers visited their students’ villages in person. The teachers held open schools in the villages, visiting in turn each village where their students lived. This method was used in response to distance education orders in areas where there was no internet signal during the COVID-19 pandemic. Another option was to move residence, as was the case of Rhidian Yasminta Wasaraka, a university lecturer from Jayapura who moved to Manokwari, West Papua. Rhidian was forced to become a “digital refugee” because her activities as a lecturer required internet access, especially because she was taking a digital short course.

8.9. Internet shutdowns also impacted the health sector. While COVID-19 pushed the health sector to use telemedicine, online consultation and spreading information using the internet, unequal or no access meant that conducting those activities was not as easy for some as they were for others.

Recommendations:

• The state should meet all of its obligations under ICCPR particularly article 19 on the right to “seek, receive and impart information and ideas through any media and regardless of frontiers”.

• The state needs to cease internet shutdowns and throttling and guarantee internet freedom for all users throughout Indonesia.