

DAWN OF DIGITAL DICTATORSHIP: WEAPONISING THE LAW AGAINST ONLINE SPEECH



"INSULTING"
PUBLIC AUTHORITIES

ITE
LAW

INDONESIA



What is the ASEAN Regional Coalition to #StopDigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship was established in 2020, by human rights and digital rights activists from Southeast Asia, on a mission to decolonize digital rights and restore our online democracies.

Together, we stand in solidarity with one another, with people from the Global Majority, resisting and pushing back against authoritarian governments and complicit tech companies.

We tell our realities from the ground, and we develop solutions together.

Our truths. Our Stories. Our Solutions. Our Liberation.

Fighting back online authoritarianism in Southeast Asia is, and shall always be, decolonial, grounded on feminist values, centred on our voices and our collective power.

Listed alphabetically, members of the Coalition include: ALTSEAN-Burma, Cambodian Center for Human Rights, ELSAM, Free Expression Myanmar, Foundation for Media Alternatives, ILGA Asia, Manushya Foundation, The Rohingya Maiyafuñor Collaborative Network, SAFEnet, Viet Tan, and Women's Peace Network.

Contact:

ASEAN Regional Coalition to #StopDigitalDictatorship

Coordination: Manushya Foundation

Email: WeAreManushyan@manushyafoundation.org

Citation:

ASEAN Regional Coalition to #StopDigitalDictatorship, Dawn of Digital Dictatorship: Weaponizing the Law against online speech in Southeast Asia, (March 2024)

Copyright

@ManushyaFoundation2024

This work is licensed under Creative Commons Attribution-NonCommercial- NoDerivatives 4.0 International Public License ("Public License"). To view a copy of this license, visit:<https://creativecommons.org/licenses/by-nc-d/4.0/legalcode>

Table of Contents

5	List of Abbreviations
7	Acknowledgements
8	Chapter I. Introduction
11	Chapter II. Methodology
13	Chapter III. Summary of International Human Rights Laws and Standards
17	Chapter IV. Country Analysis
18	4. Indonesia
18	4.1. Legal Framework
31	4.2. Challenges and Cases
49	4.3. Access to Effective Remedy
51	Chapter V. Recommendations
52	Recommendations to Governments
55	Recommendations to Members of Parliament
56	Recommendations to Tech Companies
59	Recommendations to Civil Society
60	Glossary
62	Endnote

List of Abbreviations

AJPA	Administration of Justice (Protection) Act
ASEAN	Association of Southeast Asian Nations
CCA	Computer Crime Act
CIJ	Centre for Independent Journalism
CMA	Communications and Multimedia Act
CNRP	Cambodia National Rescue Party
CPP	Cambodian People's Party
CPV	Communist Party of Vietnam
DCHCP	Department of Cybersecurity and High-tech Crime Prevention
DICT	Department of Information and Communications Technology
ESO	Electronic system operator
ETL	Electronic Transactions Law
FIDH	International Federation for Human Rights
HRD	Human rights defender
ICCPR	International Covenant of Civil and Political Rights
IFJ	International Federation of Journalists
ICJ	International Commission of Jurists
IP	Indigenous people
ISOC	Internal Security and Operations Command
ISP	Internet service provider
KPK	Corruption Eradication Commission
LPRP	Lao People's Revolutionary Party
LPSK	Witness and Victim Protection Agency
KOMINFO	Ministry of Communication and Information Technology
MCIT	Ministry of Communication and Information Technology
MCMC	Malaysian Communications and Multimedia Commission
MIC	Ministry of Information and Communication
MPTC	Ministry of Posts and Telecommunications

MPS	Ministry of Public Security
MNHRC	Myanmar National Human Rights Commission
MoI	Ministry of Information
NEC	National Election Committee
NGO	Non-governmental organisation
NIG	National Internet Gateway
NLD	National League for Democracy
OHCHR	Office of the United Nations High Commissioner for Human Rights
PAP	People’s Action Party
PAS	Malaysian Islamic Party
POFMA	Protection from Online Falsehoods and Manipulation Act
PPPA	Printing Presses and Publications Act
RGC	Royal Government of Cambodia
SAC	State Administration Council
SLAPP	Strategic lawsuit against public participation
SUHAKAM	Human Rights Commission of Malaysia
TLHR	Thai Lawyers for Human Rights
TOC	The Online Citizen
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNWGAD	United Nations Working Group on Arbitrary Detention

Acknowledgements

Manushya Foundation and the ASEAN Regional Coalition to #StopDigitalDictatorship would like to sincerely thank everyone who offered their untiring support and unique insight into the digital rights situation in Southeast Asia, and helped to make this report complete and possible.

For the section on Indonesia, we acknowledge the collaborative efforts and contributions of both Southeast Asia Freedom of Expression Network (SAFENet) as co-author and reviewer, and Manushya Foundation (co-author).

In addition, Manushya Foundation would like to express its deep appreciation to all ASEAN Regional Coalition members for their invaluable support and inputs throughout the phases of the research, from identifying the human rights issues to documenting, collecting, and analysing data for various cases, and developing this report, over the past four years. Our heartfelt gratitude extends to members, who have played critical roles in resisting digital dictatorship and advancing democratic values. Listed alphabetically, they include: **ALTSEAN-Burma, Cambodian Center for Human Rights, ELSAM, Free Expression Myanmar, Foundation for Media Alternatives, ILGA Asia, Jean Linis-Dinco, Ph.D., Manushya Foundation, The Rohingya Maïyafuïnor Collaborative Network, SAFENet, Viet Tan, and Women's Peace Network.**

Manushya Foundation and the members of the ASEAN Regional Coalition to #StopDigitalDictatorship express particular gratitude to Manushya's Digital Rights Team for their coordination, review, editing, and finalisation of the report. Overseen by Emilie Palamy Pradichit (Founder & Executive Director, Manushya Foundation), and Ni Putu Candra Dewi (Advocacy and Campaign Associate on Democracy and Digital Rights, Manushya Foundation), the team includes: Tricia Ho Sze Mei, Ploypitcha Uerfuer, Luna Marciano, Fitri Lestari, Delasari Krisda Putri, Deena Bhanarai,

and Arianne Joy Fabregas.

The visual aids within this report, including data visualisations, trend summaries, case study profiles, and theme overviews, were developed by Luna Marciano and Deena Bhanarai. Additionally, the graphics and illustrations you see would not have been possible without the patience and artistry of our designers. We extend our gratitude to Putu Deoris and Yansanjaya, who were responsible for the layout, case study design, and the creation of all the data visualisation graphics, as well as to Ivana Kurniawati, who illustrated our report and chapter cover pages.

Special gratitude is extended to the former team researchers, volunteers, and interns of Manushya Foundation, who played significant roles through their engagement in conducting desk research and monitoring cases of human rights violations over the past four years. This appreciation is particularly directed to Letitia Visan, Preeyanun Thamrongthanakij, Felicity Salina, Amalia Tihon, and Margaux Bonnard.

We also extend our deep appreciation to Ma Thida from PEN Myanmar, who made significant contributions to the work of the coalition before the illegitimate military coup in Myanmar. We extend thanks and appreciation to the numerous activists and human rights defenders across the region who have mobilised to defend fundamental human rights with immense courage, often risking their lives in the face of authoritarianism. The debt we owe them has never been greater. Their altruism and courage have been an inspiration for us and a reason more to document the gross human rights violations in the digital space.

This project would not have been possible without the help of the authors below, as well as reviewers who asked to remain anonymous, in validating our desk-research and in some cases, contributing content that informed this report.

Chapter I.

Introduction

The digital space is quickly emerging as one of the key spaces in which human rights are threatened. In Southeast Asia, the internet is no longer a free, safe, and secure space for expression. Restrictive legislation, intimidation, and even the murder of human rights defenders, activists, and journalists tarnishes the commitment to freedom of expression of the countries in the region. In this light, the need for our rights to be respected, including online, becomes greater.

This report is the outcome of the collaborative work of the ASEAN Regional Coalition to #StopDigitalDictatorship (“the Coalition”). After its establishment in 2020, with the coordination of Manushya Foundation, virtual discussions were initiated to discuss challenges faced, while determining collaborative and inclusive efforts to assess, amend, and monitor implementation of legislations affecting digital rights. The Coalition has established itself as a leading regional expert voice on digital rights in the region and is now a key player, powering local and regional voices to speak their truth to power and to resist digital dictatorship.

A core group of members of the Coalition has collectively developed the research and analysis framework of a regional ASEAN Study, which is divided into three thematic reports. This report is part of the series of three thematic reports and focuses on the right to freedom of speech and expression in the digital space.

The aim of this report goes far beyond merely analysing the legal framework related to freedom of expression online and documenting rights violations in the nine Southeast Asian countries covered. The main goal is to increase public understanding of how important digital rights are to everyone’s lives and to strengthen netizens’ knowledge of those rights. But there is more to consider. As intersectional feminists, we recognise the internet is not equal for everyone. While the digital realm offers immense opportunities, it is far from being neutral or egalitarian, and it remains susceptible to persistent backlash against the rights of women and LGBTIQ+ people. Like other social spaces, it reflects and reproduces power relations and inequalities, including those related to gender.

Coalition members dedicate their work to make Asia a safe and peaceful place for all. While they have different goals and perspectives, the cultivation of an open, safe, and inclusive digital space for all is a key priority for them. At **Manushya Foundation**, we place “equality” at the core of our activities, apply a gender lens to all of our work, and focus on powering women activists and human rights defenders, youth, and LGBTIQ+ individuals to tell their very own stories in a powerful manner for their advocacy. Likewise, **ILGA**

Asia, a regional federation of more than 204 member organisations, works for the equality of all people regardless of sexual orientation, gender identity, and sex characteristic, as well as liberation from all forms of discrimination and stigmatisation. **Women’s Peace Network** has “equality” as one of its core visions and works to protect the rights and increase the inclusion of marginalised women, youth, and communities in the Rakhine state and across Myanmar. **The Foundation for Media Alternatives** focuses on the intersection between information and communication technology (ICT) and gender rights, including tech-related gender-based violence.

We also recognise that gender inequality intersects with other forms of oppression, such as race, class, sexuality, and disability, and women exposed to intersecting forms of discrimination are particularly vulnerable to violence in the digital world. Understanding the intricate ways in which power operates, we apply an intersectional feminist lens to explore and tackle the multifaceted dynamics within the digital realm. With this report, we shed light on this and the patriarchal power dynamics that hold our world back from fulfilling a society where everyone is treated with fairness and dignity.

However, that is not where our work ends. The ultimate objective is to call, as a strong and unified voice, on governments, policy-makers, and tech companies to move the needle forward from commitments on paper to concrete measures to respect their international human rights obligations—in order to restore our only democracy. Recommendations are also extended to civil society, which provides a critical foundation for holding governments and businesses accountable, and promoting human rights and democracy.

Following **Chapter II: Methodology**, which will clarify our research and compilation process, **Chapter III: Summary of International Human Rights Laws and Standards** will provide important context for the rest of the report with a table addressing the right to freedom of expression; the rights of human rights defenders; the right to privacy; and the right to effective remedy, and indicates the ratification status by country of each convention, where appropriate. Following, **Chapter IV: Country Overviews (Analysis)** is originally split into

What is the ASEAN Regional Coalition to #StopDigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship was established in 2020, by human rights and digital rights activists from Southeast Asia, on a mission to decolonize digital rights and restore our online democracies.

Together, we stand in solidarity with one another, with people from the Global Majority, resisting and pushing back against authoritarian governments and complicit tech companies.

We tell our realities from the ground, and we develop solutions together.

**Our truths. Our Stories. Our Solutions.
Our Liberation.**

Fighting back online authoritarianism in Southeast Asia is, and shall always be, decolonial, grounded on feminist values, centred on our voices and our collective power.

nine sections, each one focused on a specific country: **Cambodia, Indonesia, Lao PDR (Laos), Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.** Each section explains how laws and legal frameworks are being used to target free expression and information online, censor or regulate content, and monitor online activities. Each section includes cases of individuals arrested and charged for their online activities, as well as instances of online censorship, monitoring, and surveillance.

However, in this booklet, the focus is solely on Indonesia.

In this booklet, a section is dedicated to the impact of COVID-19 and democracy in Indonesia. Although the pandemic has brought the world grinding to a halt, Southeast Asian governments took it as an opportunity to tighten their grip over civic space and implemented self-serving laws and policies. Under the banner of safeguarding public health, governments exploited emergency powers and other legal tools, including “fake news” laws, in restrictive and repressive ways, to advance

their authoritarian agendas, suppress freedoms and critical speech, silence political opponents, control the flow of information, and attack media freedoms. While national circumstances differed in how the pandemic was governed, the states covered in this report had national circumstances differed in how the pandemic was governed, the states covered in this report had extensive repressive powers and used COVID-19 as a pretext to limit democratic space both offline and online.

Further, each country section draws particular attention to cases of online gender-based violence and harassment experienced by women, including those who are more susceptible to online violence because of their jobs, race, religion, or identity, such as women activists and human rights defenders, women journalists, women belonging to religious or ethnic minorities, young women, women with intersecting identities (Indigenous, ethnic and minority, migrant women; lesbian, bisexual, transgender and intersex women; women with disabilities).

The report concludes with a number of **recommendations** for the primary actors identified as holding key functions in enhancing the state of digital freedoms in Indonesia, specifically that of online expression. Governments, members of Parliament, tech companies, and civil society have—each one to a different extent—a crucial role to play to uphold human rights and fundamental freedoms in the digital space. Since civil society civil groups are front and centre in representing the factual needs of the people and they can power citizens by providing civic education on human rights, a series of recommendations is likewise made to them. People are more likely to resist attempts to suppress their rights if they are aware of them.

Creating a safe internet space for everyone is crucial for promoting inclusivity, respect, and equal opportunities.

Only together can we foster a more inclusive and respectful internet culture where everyone can engage, express themselves, and participate without fear of discrimination or harassment. None of us are free until we are all free.

Chapter II.

Methodology

This Thematic Report is a culmination of four years of monitoring, research, writing, reviewing, and examining the digital rights space in nine ASEAN countries: Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, The Philippines, Singapore, Thailand, and Vietnam. Our research does not cover Brunei Darussalam and Timor-Leste due to the lack of coalition members in these countries. As mentioned previously, this booklet will, however, focus solely on Indonesia.

The methodology used in this report encompasses both primary and secondary sources. Primary data was gathered by Manushya Foundation, together with organisation members of the ASEAN Regional Coalition to #StopDigitalDictatorship. We have entrusted our coalition members to write thorough country-specific analyses, based on their expertise in the digital rights landscapes of their respective countries. It must thus also be noted that as these coalition members are specialists in their own rights, with a wealth of information obtained through lived experiences and field research, not every source will be cited, as a lot of information was first-handedly provided by the author and not obtained from elsewhere.

We included voices from the ground and experts' insight from panel discussions, including sessions we held as part of RightsCon, such as the 2022 "Thailand: Digital Authoritarianism Rising" session, the 2021 "Online Freedom Under Attack: Weaponising Misinformation, Disinformation, and 'Fake News' for Censorship in Southeast Asia" session, as well as a series of other webinars hosted by the Coalition. Participants of the webinars and discussions consisted of citizens, experts, representatives of academia, and civil society groups. For some countries, our Coalition members also conducted independent investigations and compiled data from open sources published by the relevant authorities, government agencies and the judiciary. The report's coverage spans the years 2020 through 2023, except for the chapter on Laos (**Chapter IV, 3. Lao PDR**), where

egregious human rights breaches instances prior to 2020 are also included. Similarly, for Myanmar (**Chapter IV, 5. Myanmar**) and Cambodia (**Chapter IV, 1. Cambodia**), countries for which we are also incorporating elements from 2024 due to the rapidly evolving events. We focused our inquiries on different target areas, which were ultimately synthesised into primary themes featured in the reports in this series: criminalisation of defamation and lack of human-centred cyber laws and policies; online monitoring and content moderation; threats to privacy and data protection; harassment of activists and human rights defenders (HRDs); and internet shutdowns.

This report is also composed on the basis of desk research, including a systematic literature review of relevant legislation and regulations; reports, studies, and recommendations by UN human rights mechanisms and NGOs; online news articles; policy and white papers; and independent publications. Data was also obtained from studies and external civil society organisations. We carried out interviews with a wide range of stakeholders to receive the most accurate insight on the state of digital rights on the ground relating to the target areas specified above. The study's ultimate objective is to provide a comprehensive analysis on the state of digital rights in the Southeast Asia region, including during the COVID-19 pandemic, by looking at existing national laws, policies and measures; recorded cases of violation; as well as previous recommendations or proposals made in line with international human rights laws and standards.

Chapter III.

Summary of International Human Rights Laws and Standards

Fig. G: Summary table of international human rights laws and standards.

FREEDOMS OF EXPRESSION AND TO HOLD OPINION		
International Human Rights Instruments	Relevant Provisions and Interpretations	Ratification/Voting/Adoption Date and Status
UDHR	Article 19: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law. as a matter of customary international law
ICCPR	Article 19: Upholds the right of every individual to freedom of expression, including the freedom to “seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media” without interference.	Ratified Cambodia (May 26, 1992) Indonesia (Feb. 23, 2006) Lao PDR (Sept. 25, 2009) Philippines (Oct. 23, 1986) Thailand (Oct. 29, 1996)
	Article 19(3): Articulates a three-part test, stipulating that any restrictions on expression must be “provided by law”, proportionate, and necessary for “respect of the rights and reputations of others,” “for the protection of national security or of public order, or of public health and morals.”	General comment no. 34: Article 19 (freedoms of opinion and expression): States that criminalize defamation must decriminalize it given that “imprisonment is never an appropriate penalty” for, and is neither necessary nor proportionate to the aim of protecting others. ²
UDHR	Article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law. Binding as a matter of customary international law

Fig. G: Summary table of international human rights laws and standards.(continuous)

<p style="text-align: center;">ICCPR</p>	<p>Article 17: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” It also upholds the right of persons to receive legal protection from such interference or attacks.</p> <hr/> <p>General comment no. 16: Article 17 (right to privacy): This Article is intended to protect against said infringements, both by states and private individuals. Further, “interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.” The principles of legality, necessity and proportionality also apply to privacy limitations.³</p>	<p>Ratified Cambodia (May 26, 1992)</p> <p>Indonesia (Feb. 23, 2006)</p> <p>Lao PDR (Sept. 25, 2009)</p> <p>Philippines (Oct. 23, 1986)</p> <p>Thailand (Oct. 29, 1996)</p> <p>Vietnam (Sept. 24, 1982)</p> <p>Not signed or ratified Malaysia, Myanmar, Singapore</p>
<p>Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2016) juncto Report of the OHCHR on the right to privacy in the digital age (2014)</p>	<p>Legitimate surveillance, where intended to limit the freedom of expression, requires states to demonstrate the risk that the expression “poses to a definite interest in national security or public order.”⁴ All interference with the right to privacy must also be authorised by an independent oversight body through careful review, and be accompanied with an assurance of effective remedy in case of a breach.⁵</p>	<p>Non-binding (interpretive)</p>
<p>RIGHTS OF HRDS</p>		
<p>International Human Rights Instruments</p>	<p>Relevant Provisions and Interpretations</p>	<p>Ratification/Voting/Adoption Date and Status</p>
<p style="text-align: center;">UN Declaration on Human Rights Defenders</p>	<p>Article 6: Provides for the right of persons to seek, obtain, receive and hold information about all human rights and fundamental freedoms; freely publish or impart or disseminate information and knowledge on all human rights and fundamental freedoms; and to study, discuss and hold opinions on the observance of these rights.</p> <p>Article 7: “Everyone has the right, individually and in association with others, to develop and discuss new human rights ideas and principles and to advocate their acceptance.”</p> <p>Article 9: Everyone whose rights or freedoms pursuant to the Declaration are allegedly violated must be able to access an effective remedy and have their complaint heard by an independent, impartial and competent authority.</p>	<p>NOT Binding but serves as a cornerstone for the development and evolution of international human rights law</p>

Fig. G: Summary table of international human rights laws and standards. (continuous)

RIGHT TO AN EFFECTIVE REMEDY		
International Human Rights Instruments	Relevant Provisions and Interpretations	Ratification/Voting/Adoption Date and Status
UDHR	Article 8: “Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law
ICCPR	Article 2(3): Provides for the obligation of states to ensure that those individuals whose rights have been violated have access to an effective remedy whether the violation(s) were committed by a person acting in their official capacity. Further, the effective remedy is to be determined by a competent judicial, administrative, legislative or other authority as mandated by the national legal system. The bottomline is that, regardless of the authority in charge, remedy must actually be granted.	<p>Ratified</p> <p>Cambodia (May 26, 1992)</p> <p>Indonesia (Feb. 23, 2006)</p> <p>Lao PDR (Sept. 25, 2009)</p>
	General comment no. 31 (the nature of the general legal obligation imposed on States Parties to the Covenant): Judicial and administrative mechanisms must be set in place to “investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies.” Reparation to individuals can take the forms of “restitution, rehabilitation and measures of satisfaction, such as public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices, as well as bringing to justice the perpetrators of human rights violations.” ⁷	<p>Philippines (Oct. 23, 1986)</p> <p>Thailand (Oct. 29, 1996)</p> <p>Vietnam (Sept. 24, 1982)</p> <p>Not signed or ratified Malaysia, Myanmar, Singapore</p>

Chapter IV.

Country Analysis

4. Indonesia

YEAR	DEMOCRATIC STATUS OF THE COUNTRY <small>(according to the Freedom In The World index)</small>	DIGITAL SPACE & ONLINE FREEDOM STATUS OF THE COUNTRY <small>(Digital Space Status)</small>	PRESS & MEDIA FREEDOM STATUS OF THE COUNTRY <small>(according to the World's Press Freedom Index)</small>
2020	61/100 PARTLY FREE	49/100 PARTLY FREE	119/180 (63,18) DIFFICULT
2021	59/100 PARTLY FREE	48/100 PARTLY FREE	113/180 (62,6) DIFFICULT
2022	59/100 PARTLY FREE	49/100 PARTLY FREE	117/180 (49,27) DIFFICULT
2023	58/100 PARTLY FREE	47/100 PARTLY FREE	108/180 (54,83) DIFFICULT

✓ **FREE** | Scores 100-70
⋯ **PARTLY FREE** | Scores 69-40
✗ **NOT FREE** | Scores 39-0

GOOD	SATISFACTORY	PROBLEMATIC	DIFFICULT	VERY SERIOUS
85-100 points	75-85 points	65-75 points	45-65 points	0-45 points

Fig. 4.1: Summary of freedom ratings for the Indonesia, 2020-2023.¹

4.1 Legal Framework

Freedom of Expression: Guaranteed yet Illegitimately Restricted

In Indonesia, the right to freedom of expression and speech is guaranteed by Articles 28, 28E, and 28F of the 1945 Constitution. These provisions stipulate that individuals are entitled to express themselves both verbally and in writing, and to communicate and search for, receive, possess, store, process and transmit information using all channels available.² Furthermore, Law Number 39 of 1999 on Human Rights emphasises guarantees and protection for freedom of opinion. Article 23 (2) ensures that “every person is free from holding, expressing and

widely disseminating his/her beliefs, orally or in writing through printed or electronic media, taking into consideration religious values, morals, order, public interest and nation’s unity”. Additionally, Article 25 guarantees that “every person has the right to express opinion in public, and this includes the right to strike, in accordance with the provisions of legislation”.³ The ratification of the International Covenant on Civil and Political Rights in 2006 also enhanced the protection of freedom of expression in Indonesia.⁴ These pivotal advancements underscore the heightened normative assurance for the freedom of expression in the country. Indonesia takes pride in its democratic transformation since the downfall of the

authoritarian New Order regime and its “recognition” as one of the most human rights-respecting countries in Southeast Asia.⁵ For example, unlike most in the region, Indonesia declared the offence of sedition unconstitutional in 2008.⁶ However, Indonesia is far from being exempt from digital dictatorship, as constitutional and legal guarantees are undermined by repressive laws, impacting freedom of speech and digital rights. The government persecutes its own people by using the same laws as other governments. However, due to its religious context, the Indonesian digital landscape slightly differs from most other southeast asian countries. The government places particular importance on offences against religion, and blasphemy cases are common in courts.⁷ In the end, the situation of digital dictatorship remains severe, silencing the voices of journalists, human rights defenders, and Indonesian citizens, regardless of the articles used.⁸

From Colonial Dominance to Contemporary Control: Indonesia’s Criminal Code Evolution

During our period of interest -from 2020 to 2023- the criminal code in use is none other than the century-old Dutch colonial-era legislation. This code was retained after Indonesian independence in 1945 and the enactment of the Criminal Code throughout the territory of Indonesia was officially carried out in 1958. However, on December 6, 2022, Indonesia’s parliament ratified a new Criminal Code, officially signed by the President Joko Widodo on January 2, 2023.. The new Criminal Code is scheduled to come into force three years after its promulgation, specifically on January 2, 2026.¹⁰ While this new addition could have been a boon for democracy, the new Criminal Code poses a significant threat to democratic activities and freedom of expression, both online and offline. Several controversial articles within the old and the new Criminal Code raise serious concerns that we will discuss in the following paragraphs. To enhance

readability, we will use the term “new Criminal Code” to refer to the 2023 Criminal Code (KUHP) while the term “old Criminal Code” will be used to discuss the 1946 Criminal Code.

State-Sanctioned Silence: Legal Measures Against Government and State Institutions

In the old Criminal Code, the term “defamation” is the title of Chapter XVI (Sixteen), under Article 310, a defamation claim, be it slander or libel, requires the following elements to be proven: (i) the intention of the alleged offender; (ii) harm towards the defamed party’s honour or reputation; (iii) an allegation about the defamed party charging him with a certain matter; and (iv) the obvious intent to give publicity thereof. In addition to the aforesaid elements, for defamation in the form of libel, additional elements of “writing or picture” which is “broadcasted, shown, or posted in public” must also be proven. A person being accused of defamation may put up a defence provided under Article 310 (3) of the Criminal Code, namely that such action was clearly conducted in the interest of the public or as necessary self-defence.¹¹

In addition, under the old Criminal Code, there are several types of defamation, as follows: Slander defined as verbal defamation (Article 310 (1)); Libel defined as defamation in writing (Article 310 (2)); Calumny defined as libel or slander in circumstances in which the alleged offender knowingly or maliciously issues the false statement (Article 311); Simple defamation defined as defamation that does not constitute libel or slander (Article 315); Calumnious submission of charge or information to authorities (Article 317); Calumnious insinuation (Article 318); Defamation of the dead (Article 320); and Spreading of defamation of the deceased (Article 321).¹²

Furthermore, acts within the context of defamation are also regulated in Article 142 of the old Criminal Code (defaming kings or heads of friendly countries),

Article 144 of the old Criminal Code (spreading defamation of kings or heads of friendly countries), Article 207 of the old Criminal Code (defamation of authorities or public bodies), and Article 208 of the old Criminal Code (spreading defamation against authorities or public bodies).¹³

Regarding the defamation-related articles, human rights advocates Haris Azhar and Fatiah Maulidiyanti, along with the Indonesian Legal Aid Foundation (YLBHI) and the Independent Journalists Alliance (AJI), filed a judicial review lawsuit in the Indonesian Constitutional Court. Article 14, Article 15 as well as Article 310 Paragraph (1) of the old Criminal Code have been declared unconstitutional by the Indonesian Constitutional Court in March 2024.¹⁴

However, the new Criminal Code still maintains repressive articles related to defamation. Articles 218-219 in new Criminal Code resurrect clauses prohibiting the act of insulting the president, reminiscent of *lèse-majesté* provisions crafted to safeguard the honour of a head of state in a monarchy. The language employed in the new Criminal Code specifies “attacks towards the honour and dignity of the President and/or Vice-President”, mirroring the explanation used for defamation, described as “degrading or damaging the good name or dignity, including through insults or slander”.¹⁵

These two articles were broadened by the existence of Articles 240 and 241, which extend to include insults directed at state institutions like the People’s Consultative Assembly (MPR), House of Representatives (DPR), Regional House of Representatives (DPD), Supreme Court, and Constitutional Court, deeming such acts as criminal offences.¹⁶

The existence of Articles 218-219 and Articles 240-241, indeed shows the regression of democracy, maintaining the similar provision of old criminal code. It serves as tools to stifle public criticism through legal mechanisms, impeding the exercise of the right to freedom of opinion. The presence of

these clauses can hinder societal critiques directed at the government or those in authority for the shortcomings of a prevailing system or events. This is due to the potential distortion of such criticism into an offence that falls under criminal law, posing a barrier to open expression.

Controlling Narratives: The Criminal Code’s Stance on Spreading Fake News

Despite the changes in the Criminal Code, Indonesia has consistently taken a strong stance against the proliferation of fake news. The old Criminal Code, specifically Articles 14 and 15, addressed the issue of fake news, with Article 14(1) being particularly significant as it prohibited the deliberate dissemination of false news or statements inciting societal disturbance. In July 2023, a coalition of human rights groups raised concerns about Article 14 and 15, contending that it infringed upon the state’s responsibility to uphold freedom of expression and access to information.¹⁷ This led to the Constitutional Court’s decision to annul these articles in March 2024.¹⁸ However, the introduction of the new Criminal Code has reignited discussions around fake news, as it revisits a similar provision. Articles 263 and 264 of the new Criminal Code still criminalise people who spread fake news, but with a small twist: replacing the term “disturbance” with “riot”. This recent development regarding the criminalisation of fake news shows the continued importance of advocating for digital rights. While many believe that contemporary societies equate to democracy and enhanced liberties, the reality is that these governments may not always prioritise the liberation of their own people.¹⁹

Blurred Lines: The Unsettling Landscape of Religious Blasphemy in Indonesia

Indonesia has multiple criminal provisions concerning blasphemy, with the most well-known is the so-called Blasphemy Law (Presidential Instruction

No. 1/PNPS/1965 on the Abuse and Defamation of Religion). Article 4 of this brief presidential instruction inserted an article on blasphemy into the old criminal code, under Article 156a. The article 156a of the old Criminal Code regulates the blasphemy and religious defamation with punishment up to five years in prison.²⁰

The new Criminal Code has not eliminated blasphemy, even maintaining the provision. Articles 300-305 of the new criminal code extend the scope of the 1965

blasphemy law, established during President Soekarno's tenure. Previously, there was only a single article that "protected" six officially recognized religions in Indonesia: Islam, Protestantism, Catholicism, Hinduism, Buddhism, and Confucianism. The new code broadens the law's coverage because it adds the word *kepercayaan* (belief) to what is covered under the 1965 law. Article 302 states that if a believer becomes a non-believer, that is apostasy and that anyone who attempts to persuade a person to be a non-believer is committing a crime.²¹

#PeoplePower | How Are People Resisting Digital Dictatorship?

In the Face of Silence: People Power and Civil Society's Battle for Freedom in Indonesia

While the legislative framework in Indonesia may be discouraging, Indonesians do not lose hope and continue to fight against these restrictions on freedom of expression. Among these efforts, a coalition of legal experts and civil society groups united in December 2022 as the National Alliance for Criminal Code Bill Reform to thwart the passage of the Criminal Code Bill. Through concerted efforts, they scrutinised the bill's provisions and engaged with various media outlets to raise awareness about its potential impact. Their primary concern centred on the threat to freedom of expression posed by certain provisions, which they deemed regressive and likely to roll back democratic gains made since Suharto's departure in 1998. By mobilising public opinion and advocating for democratic principles, the coalition aimed to defend fundamental rights and preserve Indonesia's democratic trajectory. At the same time, on December 5, 2022, the Press Legal Aid Society (known as LBH Pers in Bahasa Indonesia) organised a protest outside the House of Representatives against the enactment of the Criminal Code, citing concerns about threats to press freedom. Journalists expressed apprehension about the potential criminalisation they may face under Article 263, which addresses the dissemination of misinformation without providing clear criteria for what constitutes false information. This ambiguity raised fears among press members regarding the risk of undue legal action. The protest garnered widespread support from diverse groups, including NGOs, legal aid organisations, indigenous communities, students, labour unions, environmental activists, and women's rights advocates.²² This illustrates how Indonesians are keenly aware of their country's policies and are quick to stand up for their own interests. It shows that when needed, people from different backgrounds come together to protect their rights and freedoms, highlighting a strong sense of community and democracy, where everyone has a voice in shaping the country's future.



International Critique from United Nations Special Rapporteur

Prior to the president's approval in November 2021, Mary Lawlor, UN Special Rapporteur on the situation of human rights defenders, delivered a scathing condemnation of Indonesia's criminalisation of defamation. Lawlor's forceful critique laid bare the intentional targeting of civil society organisations merely for fulfilling their essential roles. Arguing passionately for a paradigm shift, she asserted that defamation should be considered a civil matter, not a criminal offence—a sentiment echoed by various UN bodies advocating for the removal of defamation from Indonesia's criminal code. Lawlor's stark warning resonates:

“

I am extremely concerned at the way defamation laws are being used in Indonesia to undermine the right to freedom of opinion and expression.²³

- Mary Lawlor, UN Special Rapporteur on the situation of human rights defenders

#PeoplePower | How Are People Resisting #DigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship Takes a Stand: Unyielding Advocacy for Digital Freedom in Indonesia and Beyond. ²⁴

The ASEAN Regional Coalition to #StopDigitalDictatorship, standing in solidarity with the Indonesian people, vehemently condemned the government's criminalisation of defamation. The coalition called for an immediate repeal of the criminal defamation provisions within the Penal Code, urging an end to the harassment and suppression of freedom of expression.

The coalition continues to urge the Indonesian government to overhaul repressive laws that hinder the protection of freedom of expression. A crucial call echoes, emphasising the need to align these laws with international human rights standards for the unequivocal protection of fundamental freedoms. The coalition deems the criminalisation of defamation inherently disproportionate and an unnecessary restriction on the right to freedom of opinion and expression, as mandated by international human rights law.



The coalition's demands extend further, pressing the Indonesian government to annul any other laws and regulations that infringe upon fundamental freedoms in ways incongruent with international standards. Their uncompromising stance underscores the urgent need for legal reforms aligning with the principles of liberty and human rights.

In a resounding declaration, the ASEAN Regional Coalition to #StopDigitalDictatorship strongly condemns all actions by the Indonesian government that violate human rights. Emphasising the indispensable right of the Indonesian people to freely express themselves both offline and online, the coalition stands as a formidable advocate for digital freedom in the ASEAN region. The struggle in Indonesia becomes emblematic of a broader regional fight against oppressive measures, echoing the collective cry for unrestricted freedom of expression.

Undermining Freedom: Law on Electronic Information and Transactions (ITE Law)

When discussing digital rights in Indonesia, it's essential to address the Electronic Information and Transactions Law (ITE Law). First enacted in 2008, it has been amended several times since, with the first amendment in 2016 and the latest (second amendment) in early 2024. The ITE Law

is a comprehensive legal framework designed to regulate a wide array of aspects related to electronic transactions within Indonesia. Enacted to keep pace with the rapid advancements in digital technology, this law addresses the increasingly prevalent online transactions, encompassing both commercial and

non-commercial activities. In addition, the ITE Law also incorporates provisions aimed at combating cybercrime. These provisions target various forms of illicit activities occurring in cyberspace, including hacking, unauthorised access to computer systems, and the dissemination of illegal content. One of the notable aspects of the ITE Law is its applicability to a broad spectrum of stakeholders, including individuals, businesses, and governmental entities, engaging in electronic transactions. However, the ITE Law has sparked debates and controversies, particularly concerning its potential impact on freedom of expression. Certain provisions within the law, notably defamation, hate speech, and the dissemination of false information, have drawn criticism for their perceived overreach and ambiguity. Critics argue that these provisions pose a risk of being weaponised to suppress dissenting voices intensify the threat to public access to information.²⁵

Weaponising Defamation: Unveiling the Threat in Indonesia’s ITE Law

Under the original version of the ITE Law, Article 27 (3) prohibits the distribution, transmission, and/or granting of access of electronic information and/or electronic documents with offensive and/or defamatory content.²⁶ However, the original version of the ITE Law did not provide a clear definition of content that could be deemed insulting or defamatory.²⁷ While, the Second Amendment of the ITE Law, in Article 27A, it is defined as intentionally attacking the honour or good name of another person by accusing them of something, with the intention of making the matter known to the public through electronic information or electronic documents via an electronic system.²⁸ It remains a flexible provision with the potential to criminalise critical communities.

Historically, the ITE Law has been weaponised to silence human rights defenders, academics, and commoners. Between January 2019 and December 2022, Amnesty International Indonesia documented

over 1,021 cases where human rights defenders faced prosecution, arrests, attacks, and threats under the defamation article in ITE Law.²⁹

Combating Fake News: Ambiguities and Threats to Expression

In the original version of the ITE law, Articles 28 and 45 A(3) address hoaxes and hate speech online, imposing severe penalties of up to six years in prison and a fine of IDR 1 billion (\$66,884). Article 28(1) prohibits the act of “disseminating, knowingly and without title, false and misleading information resulting in injury to customers of “[e]lectronic [t]ransactions.”³⁰ Criminal hate speech can likewise be found in Article 28(2), which proscribes the spreading of information with the intention of provoking hate or enmity among individuals or groups based on their ethnicity, religion, race or group identity. Despite these clauses being intended to reinforce user protection and prevent hate crimes respectively, they are extremely susceptible to erroneous and expansive interpretations: “false information” and “hate speech,” for instance, could be understood in many different ways depending on their context.³¹ This ambiguity becomes even more concerning in light of the questionable integrity of the Indonesian judiciary and law enforcement.

In the Second Amendment of the ITE Law, Article 28(3) was introduced, stating, “Everyone knowingly disseminates Electronic Information and/or Electronic Documents that he knows contain false notifications that cause riots in society.” This addition raises even more concerns than the previous version, as it introduces ambiguity and potential for abuse. This article lacks clarity in defining what constitutes a “false notification,” leaving it open to subjective interpretation. Consequently, there is a heightened risk of misuse and selective enforcement, as individuals or authorities may exploit the vague language to suppress dissenting opinions or target individuals or groups based on political or ideological differences.

The Second Amendment of ITE Law: Enabling an Arbitrary State

Before the Second Amendment of the ITE Law, the role of the government in regulating the digital sphere was not clearly defined, leaving a dangerous ambiguity regarding its authority over online content and electronic systems. However, with the introduction of Article 40 and 40A in the amended law, the government's powers have expanded significantly. Prior to the amendment, there was no specific provision granting the government authority to block access to online content or terminate electronic system access based on subjective determinations of legality or decency. After the amendment, particularly in Article 40 (2b) and (2bB), the government is explicitly and legally empowered to take such actions, including blocking access to content it deems defamatory or unlawful and ordering Electronic System Operators to comply. This significant shift grants the government unprecedented control over online information and communication channels.³²

Revictimisation Risks and Legal Ambiguities: Implications on Women and Freedom of Expression

Article 27 (1) of the original version of the ITE law and the Second Amendment of the ITE Law has legal ambiguities, particularly for women who are victims of sexual violence. The indiscriminate transmission of electronic evidence puts them at risk of unjust criminalisation instead of recognition as victims of harassment or violence. This vulnerability allows perpetrators to exploit legal gaps, leading to a dual-layered violence – first offline and then facilitated by technology.³³

An illustrative case is that of Mrs. Baiq Nuril Maknun in Lombok, who, after facing sexual harassment, found herself prosecuted under the ITE Law in 2018, by her perpetrator, H. Muslim. This attempt to criminalise her, utilising Article 27 (1),³⁴ goes against

Indonesia's obligation under UN CEDAW's Article 2 to eliminate discrimination against women.³⁵ In 2019, President Joko Widodo granted amnesty to her. Despite this, the Indonesian government, by maintaining Article 27 (1), fails to protect victims who preserve electronic evidence of harassment and violence, as well as those who speak out on social media. This contradicts its obligation to prevent gender-based violence.

#PeoplePower | How Are People Resisting #DigitalDictatorship?

Resisting Repression: People Power Against the Second Amendment of the ITE Law

The Serious Coalition for Revision of the ITE Law vehemently rejects the Second Amendment, citing a lack of meaningful public participation and the perpetuation of articles threatening freedom of expression.³⁶ The coalition also highlighted the closed nature of the revision process, leaving little room for public involvement and oversight. This lack of transparency poses a major risk of potentially resulting in regulations that benefit elites rather than protecting human rights.³⁷

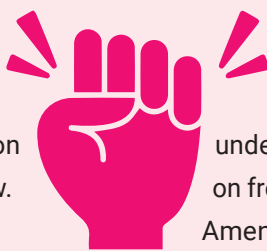


Defying Oppression: The ASEAN Regional Coalition's Fight Against Censorship in the Second Amendment of the ITE Law.³⁸

The ASEAN Regional Coalition to #StopDigitalDictatorship stands in solidarity with Indonesian civil society, vehemently condemning the Indonesian government's stance on the criminalisation of defamation, hate speech, and false news. The coalition advocates for the immediate repeal of these provisions within the Penal Code and the ITE law, emphasising the imperative to uphold the principles of freedom of expression as per international human rights law.

The coalition urgently calls on the Government of Indonesia to fulfil its obligations to uphold, respect, and protect freedom of expression and opinion, as outlined in Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and

Political Rights (ICCPR). Critically, the Second Amendment of the ITE Law is criticised for lacking transparency, open governance, and meaningful public participation, ultimately failing to adhere to the foundational principles crucial for a thriving democratic society. Furthermore, expressing regret over the lack of transparency and accountability during the revision process, the coalition underscores the persistence of restrictions on freedom of expression within the Second Amendment of the ITE Law. In the spirit of true democracy, the coalition advocates for open discussions to be encouraged, fostering a diversity of opinions and ensuring that legislative decisions are well-informed and representative of the public interest.





The draft criminal code and provisions in the ITE Law in Indonesia pose significant problems, as they have the potential to harm numerous victims and hinder critical discourse. These regulations also risk unjustly criminalizing survivors of sexual violence, which is deeply concerning. To address these issues, it is crucial that revision efforts actively involve the participation of these victims. By including their voices, policymakers can ensure that fear is not perpetuated and that freedom of expression is not unjustly limited. The Community of Victims of the ITE Law, or PAKU ITE, strongly urges policymakers to listen to the voices of the victims and prioritise the protection of citizens' rights. It is important to view laws as instruments for safeguarding individuals' well-being and promoting a just society, rather than as tools of suppression. By centering the experiences and perspectives of those affected by these laws, policymakers can make informed decisions that uphold human rights and foster an environment of inclusivity, justice, and freedom of expression.

- Anindya Shabrina, Deputy Chair of PAKU ITE

What is MR5 and its amendment MR10 ?

This ministerial regulation signed in 2020 and amended in 2021, raises significant concerns as it grants government authorities excessively broad powers to regulate online content, access user data, and penalise non-compliant companies.

Companies are mandated to “ensure” that their platforms are free from “prohibited content”, implying a requirement for active content monitoring. Failure to comply may result in the blocking of the entire platform, raising issues of prepublication censorship.

KOMINFO will sanction non-registrants by blocking their services. Private ESOs choosing to register must provide information granting access to their “system” and data, essential for effective “monitoring and law enforcement”. Any disobedience, such as a failure to provide ‘direct access’ to systems (Article 7 (c)), can lead to various penalties, including warnings, temporary blocking, full blocking, and, ultimately, the revocation of registration.³⁹

Silencing Cyberspace: The Chilling Impact of MR5 and its amendment MR10 on Freedom of Expression in Indonesia

MR5 and Its Amendment MR10 on Freedom of Expression in Indonesia: Unravelling the Controversial Regulatory Web Since 2020.

On November 16, 2020, the Ministry of Communication and Information Technology (KOMINFO) issued Regulation Number 5 of 2020 on Private Electronic System Operators (ESOs) (hereinafter MR5). Further, in May 2021, it was amended with its Ministerial Regulation Number 10 of 2021 (MR10) to include over-the-top (OTT) services, such as messaging apps and voice over IP (VoIP) services.⁴⁰

This instrument grants authorities unfettered powers to regulate online content and force social media platforms, apps and other service providers to register with KOMINFO through a designated portal and provide access to any stored user data on their systems. Failure to comply with this requirement would lead to blocking of the entire platform.⁴¹

Companies must “ensure” that their platform does not contain or facilitate the distribution of “prohibited content,” which implies that they have an obligation to monitor content.⁴² Failure to comply with this requirement would lead to blocking of the entire platform.⁴³ This new regulation will affect national and regional digital services and platforms, as well as multinational companies like Google, Facebook, Twitter, and TikTok.

This regulation is one of the most controversial regulations passed by President Widodo’s administration; aside from condemnations by local and international human rights groups, a petition circulating online since early 2022 that calls for its repeal has been signed by no less than 11,000 netizens.⁴⁵

#PeoplePower | How Are People Resisting #DigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship urges Indonesia to repeal Ministerial Regulation Number 5 Year 2020 (MR5) and its amendment, Ministerial Regulation Number 10 Year 2021 (MR10)⁴⁶

The regulation introduces content moderation provisions inconsistent with internationally recognized human rights, including freedom of expression. The coalition stresses that MR5 and its amendment MR10 exacerbate existing challenges for freedom of opinion and expression, severely impeding internet freedom through excessive penalties for non-compliance. Expressing concerns, the coalition notes the government's inadequate response to problems hindering online freedoms and the heightened risk of judicial harassment faced by citizens, particularly human rights defenders. MR5 and MR10, with their authoritarian enforcement, disrupt the civic space, erasing crucial channels for online expression. Failure to register will result in blocking, limiting Indonesians' ability to access information freely—a right protected by international human rights treaties and principles.

The coalition emphasises the insufficient public participation in developing legislation, policies,

and implementing guidelines related to MR5 and its amendment MR10. Despite falling under KOMINFO's lawmaking authority, public participation remains essential. Pressing further, the coalition asserts that Indonesia has neither improved its response to issues hindering such freedoms nor addressed the associated risk of judicial harassment faced by citizens, especially human rights defenders, expressing themselves online.

The coalition stresses that MR5 and its amendment MR10, with their authoritarian enforcement against private ESO, seriously disrupt the civic space, erasing key channels for individuals to exercise their online freedoms. Private ESOs that fail to register will be blocked in Indonesia. To date, major platforms have not registered or shown any intention to do so. Their refusal, resulting in service-blocking, substantially limits Indonesians' ability to access information freely—a right protected by human rights treaties and principles to which Indonesia is bound.



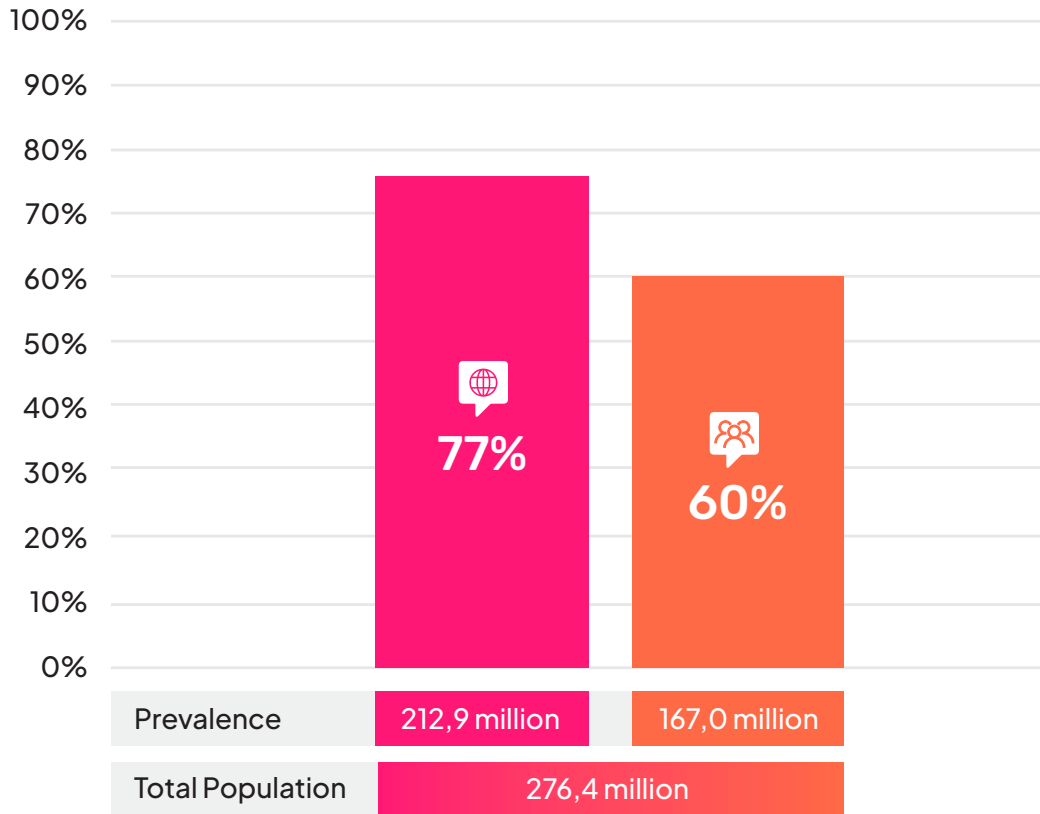
Indonesia Percentage of Internet and Social Media Users



Internet Users



Social Media Users



DataReportal, *Digital 2023, Indonesia*, (9 february 2023), available at : <https://datareportal.com/reports/digital-2023-indonesia>

Fig. 4.2A: Percentage of Internet and Social Media Users in Indonesia, 2023.

4.2 Challenges and Cases

Struggles, Legislation, and Repression in Indonesia (2020–2023)



LEGEND:

⚠️ : Alleged offense + (articles/provisions invoked against the individual)
 - "Unknown": Either information is not available or no articles/provisions have been cited by the judiciary

🔒 : Legal and extralegal consequences
 - "Status Unknown": Current status of the individual is unknown (detained, convicted, deceased, etc).

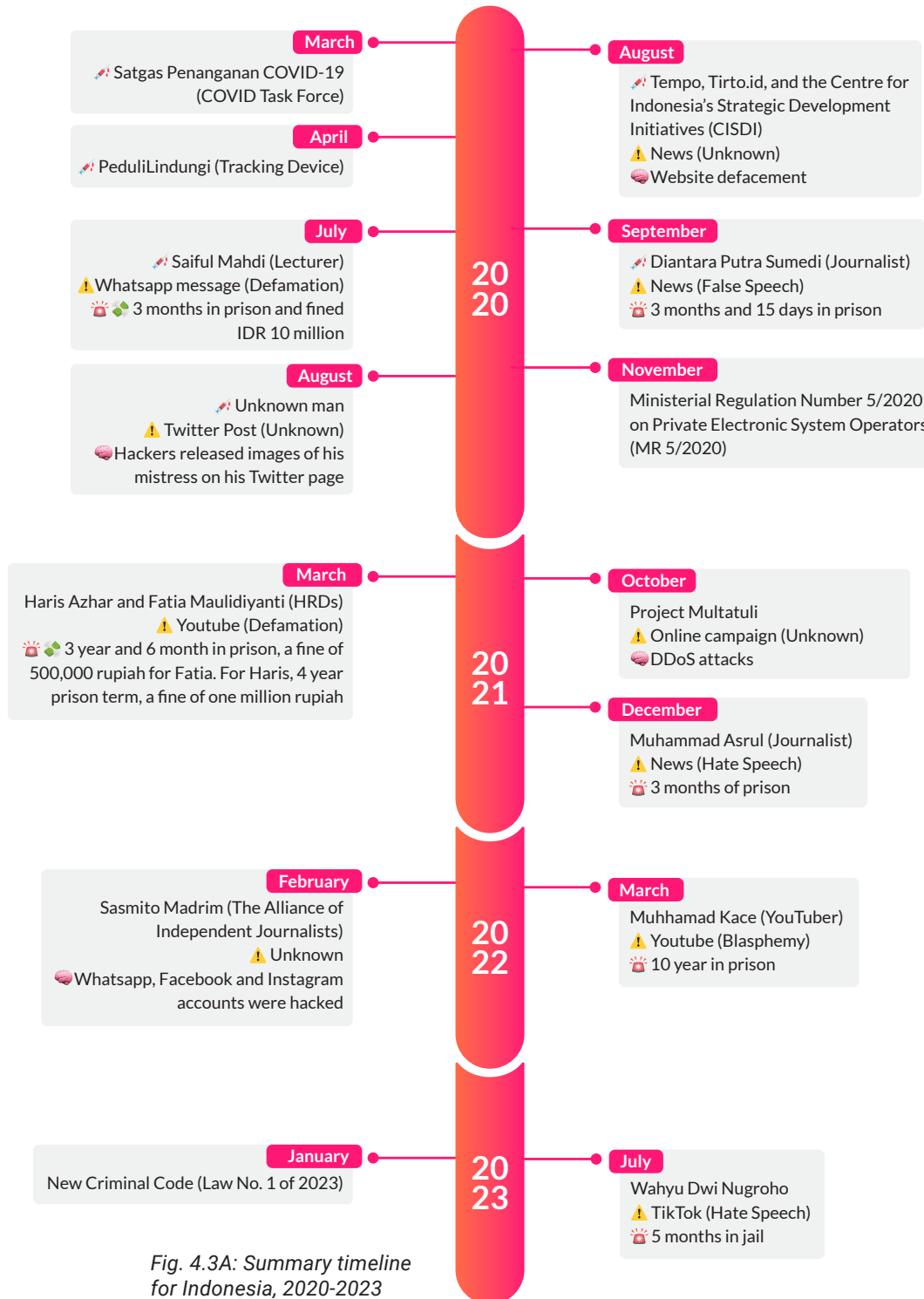


Fig. 4.3A: Summary timeline for Indonesia, 2020-2023






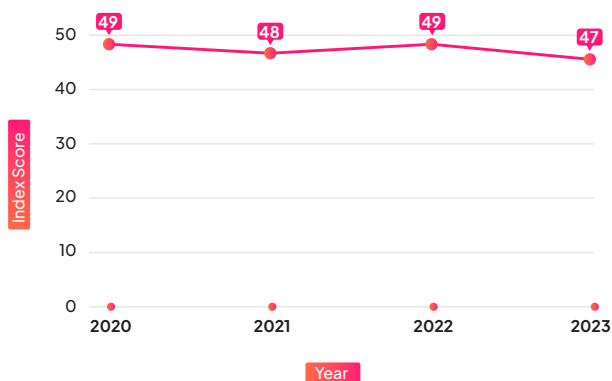
Country	Event	Contextualisation
 INDONESIA	 Ministerial Regulation Number 5/2020 on Private Electronic System Operators (MR 5/2020)	The regulation gives the Indonesian Ministry of Communications and Information Technology (MoCI) broad powers to block and restrict access to online content deemed inappropriate or harmful, without clearly defining the criteria or procedures for determining what constitutes a violation.
	 New Criminal Code (Law No. 1 of 2023)	The New Criminal Code stipulates harsh penalties for speech-related offenses including the dissemination of false information, insults, defamation, and the promotion of abortion.
	 Presidential Instruction No. 1/PNPS/1965 on the Abuse and Defamation of Religion	This legislation has been used to incorporate a provision on blasphemy into the penal code. It stipulates penalties of up to five years' imprisonment for individuals who deliberately and publicly exhibit sentiments or actions that are derogatory, disrespectful, or offensive towards a religion embraced in Indonesia, with the aim of dissuading others from adhering to any faith centered on belief in the One God.
	 Law on Electronic Information and Transactions (ITE Law)	Despite the Indonesian government's effort to revise the ITE Law, several problematic articles, including those concerning defamation, hate speech, and false news, have systematically hindered the fundamental right to freedom of expression and have silenced advocates for human rights.

Fig. 4.3B: Contextualisation for Indonesia's timeline, 2020-2023.

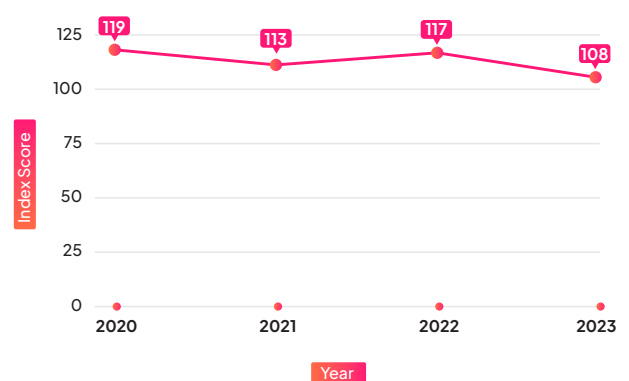
Various indices suggest the rise of digital dictatorship in Indonesia in recent years. Freedom on the Net ranked Indonesia "partly free" with an aggregate score of 48/100 in 2021, score of 49/100 in 2022 and a score of 47/100 in 2023.⁴⁷ Indonesia placed 117th out of 180 countries on Reporters Without Borders' 2022 World Press Freedom Index, with a score of 49.27 and placed 108th out of 180 countries on Reporters Without Borders' 2023 World Press Freedom Index, with a score of 54.83.⁴⁸

Digital Space & Online Freedom Status (Freedom on The Net)



Freedom House, *Explore the Map*, (n.d.), available at: <https://freedomhouse.org/explore-the-map?type=fiw&year=2023>

Media & Press Freedom (World Press Freedom Index)



Reporters sans frontières, *Classement*, (n.d.), available at: <https://rsf.org/fr/classement>

Fig. 4.4: Digital Space & Online Freedom Status (Freedom on The Net) and Media & Press Freedom (World Press Freedom Index) Ratings for Indonesia over the years, 2020-2023.

A Worrying Increase in Online Reports Based on Defamation

The Indonesian National Police has a special Cyber Crime Unit who is tasked with handling reports of computer and computer-related crimes. According to data published on the Unit’s website, the number of reports they receive is consistently increasing.⁴⁹ The Indonesian House of Representatives also revealed that some 3,500 reports were received by the Unit in the first quarter of 2021 alone.⁵⁰ By the end of that year, a tally released by the Unit showed that the figure had climbed to 4,080. However, this data is neither final nor accurate as it does not line up with the breakdown provided in Table 1 below.⁵¹

According to a breakdown of these numbers based on the type of offence, defamation is the most commonly reported, followed by indecency and hate speech. Meanwhile, fake news reports had a significant jump between 2019 and 2020, a period that coincides with the coronavirus outbreak. Full data from 2021 is unavailable, although we were able to fetch figures of cyber threat and fake news reports.⁵²

YEAR	DEFAMATION	HATE SPEECH	INDECENCY	CYBER THREATS	FAKE NEWS
2020	1,479	223	404	135	197
2021	N/A	N/A	N/A	5,276	414
2022	N/A	N/A	N/A	4,860	N/A
2023	838	N/A	N/A	3,758	N/A

Fig. 4.5: Breakdown of reports based on offence type, Indonesia, 2020-2023.

The notable surge in reported cases, particularly during 2020, predominantly concerning defamation and hate speech, serves as compelling evidence of the escalating constraints on online speech and expression in recent years. While there is a decrease in defamation reports, we still need to examine whether this indicates a genuine reduction in actual incidents or if, in reality, the dark figure has increased. It could be changes in reporting mechanisms, public awareness, or legal frameworks, given Indonesians must often practise self-censorship and refrain from speaking up against or criticising the government. It was also revealed that a good portion of those reports were submitted by individuals who are in a position of power, such as public officials, professionals and affluent persons.⁵³

Everybody is At Risk of Being a Target of the Government

In 2020, SAFEnet documented 22 cases of internet users being charged with Article 27(3) of the ITE Law. An additional 17 were reported in 2021.⁵⁴ Data gathered by Amnesty International Indonesia, conversely, shows that the ITE Law was used against approximately 81 people from January 2020 to October 2021, most of whom were accused of defamation.⁵⁵ Between January 2019 and December 2022, Amnesty International Indonesia documented that at least 1,021 human rights defenders faced prosecution, arrests, attacks, and threats, under the defamation article in ITE Law.⁵⁶ SAFEnet has also highlighted a concerning trend, reporting a total of 89 cases of criminalisation related to these articles from January to October 2023.⁵⁷ These findings

support the longstanding observation of activists and HRDs that the ITE Law is routinely misused to criminalise hundreds of people simply for exercising their right to freedom of expression online.⁵⁸ A 2023 report by FORUM-ASIA and KontraS shows a new pattern in officials' efforts to suppress criticism: Cease-and-Desist letters. Started in 2021, this type of action consists of public officials redacting letters in which they fill in for lawsuits against activists, often citing defamation, insults, or fake news. The approach often ends in criminalisation, with the accused facing charges and further pressure from the government to cease their activism. This also occurred in Haris Azhar and Fatia Maulidiyanti's cases detailed below.⁵⁹

“

Despite by the end of 2023 the ITE Law having been amended or revised twice, the defamation and blasphemy articles, which have often been misused to silence criticism and repress press freedom, are still maintained. In fact, now new articles have been added, such as articles prohibiting disinformation and excessive authority to cut off Internet access, making the ITE Law even more dangerous for the future of Internet freedom and democracy in Indonesia. It is easy to imagine the number of judicial harassment cases increasing and online censorship becoming more rampant.

- Damar Juniarto, Executive Director of SAFEnet 2018-2023 and Advisor of SAFEnet

March 2020 saw the prosecution of Mohamad Sadli, chief editor of online news outlet Liputan Persada. Sadli was charged with hate speech and defamation, and sentenced to two years for an opinion piece he wrote which criticised a road construction project backed by the local government.⁶⁰ Just less than a month later, Saiful Mahdi, a university lecturer at Syiah Kuala University in Banda Aceh, was handed a three-month sentence and fined IDR 10 million (\$668) under Article 27(3) of the ITE Law for his WhatsApp messages criticising the university policy on staff recruitment. The Supreme Court upheld his guilty verdict on June 29, 2021 and Mahdi began to serve his time in September.⁶¹ He was granted a presidential pardon after one month.⁶² Article 27(3) of the ITE Law was also used against activist and urban planning expert Marco Kusumawijaya in February 2021. He was accused of defamation after posting on Twitter that a residential area in North Jakarta looted sand from the shores of Bangka Belitung, his hometown, during its development phase.⁶³ His case was closed. In October 2021, Marco posted screenshots of a Google alert he received showing that potential government-backed attackers were attempting to hack his email account.⁶⁴

Another example is the case of Alvoaria Reba, a Papuan activist behind “Qvarica,” a Facebook account associated with the Free Papua Movement. In April 2020, she was sued by the West Papua Provincial Government’s legal team for having allegedly insulted the Governor of West Papua on social media. The allegation stemmed from a post in which she expressed her disagreement with the closure of Rendani Manokwari Airport. She now faces defamation charges carrying a maximum sentence of four years and/or a fine of up to IDR 750 million (\$50,163).⁶⁵

In April 2021, a labour union leader by the name of Stevanus Mimosa Kristianto was charged under

Article 310(1) of the Criminal Code and Article 27(3) of the ITE Law on allegations of defamation against Maybank Indonesia after a speech he had delivered while protesting against the bank appeared in an online news article.⁶⁶ The same two laws were used against HRDs Haris Azhar and Fatia Maulidiyanti, both of whom were subpoenaed by Minister for Maritime Coordination Luhut Binsar Panjaitan and threatened with a lawsuit in August 2021. The case emerged following a talk show featured on Azhar’s YouTube channel titled “Ada Lord Luhut di balik Relasi Ekonomi-Ops Militer Intan Jaya!! Jenderal BIN juga Ada!!” (There is Lord Luhut behind the relation of Economy-Military Operation Intan Jaya!! The General of State Intelligence Agency is also there!!) in which he and Maulidiyanti discussed findings in a multi-stakeholder report revealing the involvement of Indonesian army officials and retirees in an extractive gold mining project in Papua.⁶⁷ On Sept. 22, the Minister filed a complaint against both persons and demanded each to pay him IDR 100 billion (\$7 million) in compensation.⁶⁸ On Jan. 18, 2022, they were summoned for questioning by the Greater Jakarta Police Department, where they had to answer a total of 37 questions on the details of the case and their activism over six hours.⁶⁹ By March 18, they were officially named suspects and as of March 2023, they face defamation charges which could lead to imprisonment for up to four years if convicted.⁷⁰ Since April 3, 2023, Fatia and Haris have undergone 31 hearings. On November 12, during the indictment reading at the 28th hearing, the lead prosecutor recommended a three-year and six-month prison sentence for Fatia, along with a fine of IDR 500,000 (\$32).⁷¹ For Haris, the prosecutor advised a four-year prison term, accompanied by a fine of one million rupiah (\$65). It’s noteworthy that the latter penalty represents the maximum punishment stipulated under the ITE law. The adjudication of the final judgement is scheduled to take place in the second week of January 2024.⁷²

INDONESIA

2023 Political Overview

Parliamentary Presidential system in theory, semi-authoritarian regime in practice.

Head of Government

President Joko Widodo

#FreeFatiaHaris

📖 🗣️ 🌱 CASE STUDY

Digital Dictatorship used to silence **Indonesian activists** fighting for **corporate accountability** and **climate justice**...

WHO

❤️ Fatia Maulidiyanti, an Indonesian HRD, and coordinator of KontraS

Haris Azhar, an Indonesian HRD, educator, and ED of Lokataru Foundation

WHY/WHAT

🗣️ 🌱 Targeted by authorities for releasing a YouTube video featuring them discussing ways in which gold mining corporations and the Indonesian military were complicit in exploitative practices at the Blok Wabu site in Intan Jaya, Papua.

🗣️ Fatia and Haris assured that their data was well-researched and backed up by various studies performed by multiple CSOs. Nevertheless, the Coordinating Minister for Maritime and Investment Affairs accused them of spreading false news, and defamation.

WHEN

20 August 2021 (content posted); 22 September 2021 (charged); 13 November 2023 (sentences administered); 8 January 2024 (acquittal)

WHERE

Blok Wabu, Intan Jaya, Papua (gold-rich land that Fatia and Haris were raising awareness about)

HOW

⚠️ How Digital Dictatorship has caused the violation of Fatia and Haris' human rights:

Fatia and Haris were charged with slander and defamation (**under Articles 310 and 311 of the Criminal Code**) and for violating the **amended Electronic Information and Transaction (EIT) Law (Article 45(3))**.

- 🗣️ 🌱 Fatia: Sentenced to 3 years and 6 months in prison. Fined 500,000 rupiah.
- 🗣️ 🌱 Haris: Sentenced to 4 years in prison. Fined 1,000,000 rupiah.

🗣️ Both faced judicial harassment for many years. Both were acquitted in early 2024.



Haris Azhar

Indonesian HRD, educator, and ED of Lokataru Foundation

Fatia Maulidiyanti

Indonesian HRD, and coordinator of KontraS

Manushya Foundation, Joint Statement Indonesia: Solidarity for Human Rights Defenders Fatia Maulidiyanti and Haris Azhar, (22 November 2023), available at: <https://www.manushyafoundation.org/fatiaharisglobalsolidarity>

Forum-Asia & KontraS, Indonesia: Human rights groups celebrate the acquittal of human rights defenders Fatia Maulidiyanti and Haris Azhar, calls for repeal of defamation laws, (2024), available at: <https://www.forum-asia.org/wp-content/uploads/2024/01/Joint-Statement-Indonesia-Fatia-Haris-2024.pdf>

Arrests, litigation, and the other forms of harassment mentioned in this case study are just some examples of how Digital Dictatorship has affected the individual(s) mentioned, as well as Southeast Asian society as a whole. HRDs and/or journalists, including the one(s) in this case study, are often perpetually targeted by Digital Dictatorship in numerous ways that go beyond just what is discussed here.

“

In light of similar cases, the criminalisation [of Azhar and Fatia] inevitably attests to the tendency of public officials to perceive criticisms as a personal attack.⁷³

- Robertus Robet, human rights activist and member of the Indonesian Caucus Advisory Council for Academic Freedom (KIKA)

According to Amnesty International, in Indonesia, at least 35 cases of physical and digital attacks involving 150 human rights activists and organisations were reported in 2022.⁷⁴ In April, YouTuber Muhhamad Kace was sentenced to ten years in prison after being accused, in 2021, of allegedly posting blasphemous content online insulting the Islam religion.⁷⁵ A similar case happened during the same month, when Ferdinand Hutahaeen, a former Christian who converted to Islam, was given five months imprisonment after being accused of spreading false information, including a Tweet about Islam.⁷⁶

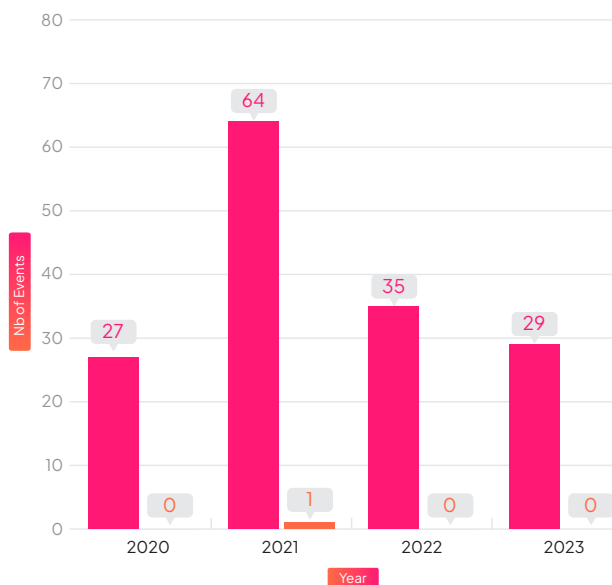
The Alliance of Independent Journalists (AJI) Indonesia's chairperson was hacked on multiple platforms in February 2022. Sasmito Madrim's Whatsapp, Facebook and Instagram accounts were

hacked simultaneously: he was unable to receive calls and messages and had his profile photo changed into a pornographic image. Furthermore, false information was posted on his accounts which supported the arrest of HRDs Fatia and Haris, as well as the construction of the Bener Dam in Purworejo, Central Java, in an attempt to alienate AJI from other civil society organisations.⁷⁷

False News and Hate Speech: A Pretext for the ITE Law and MR5 to Censor Free Speech

Aside from defamation, ITE Law provisions on false news and hate speech are also often cited in cases against netizens. Out of 84 online speech-based convictions SAFEnet recorded throughout 2020, 64 were delivered based on at least one (or a combination of) those articles within the ITE Law.⁷⁸ In 2021, the total number of convicted persons dropped to 38, of which 10 were activists, the highest since the ITE Law came into effect.⁷⁹ In 2022, a total of 97 cases of criminalisation were documented, affecting 107 victims. The primary articles used to prosecute the defendants predominantly pertained to ITE Law.⁸⁰ The number of complaints in 2023 increased by 15.9 percent, with a total of 126 people in 114 complaints reported to the police. 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 businesses. (https://mega.nz/file/skVBwQQL#yPYVShJLSY-M3OH04gRZ3ZcU9aAGYNBMx00vP0Cd_XRs). Article 28(2) of the ITE Law on hate speech was used against, amongst others, Muhammad Asrul, a journalist of online news outlet Berita News. He was detained for 36 days after publishing three articles covering a corruption scandal involving the son of the mayor of Palopo, a city in South Sulawesi.⁸¹ Asrul was sentenced to three months by the Palopo District Court on Nov. 23, 2021.⁸² On Aug.

Disorders involving the Media in Indonesia



The Armed Conflict Location & Event Data Project (ACLED), *Disorder Involving the Media*, (10 February 2024), available at: <https://acleddata.com/data-export-tool/>



Fig. 4.2B: Disorders involving the Media in Indonesia, 2020-2023.



The information used to construct this infographic is sourced from the ACLED database, specifically the dataset titled "Disorders involving Media." Within this database, we have exclusively selected relevant countries from the ASEAN region, namely Indonesia, Thailand, Myanmar, and the Philippines. However, this infographic only focuses on Indonesia. The events were further filtered based on an additional criterion: date. As our report focuses on events from 2020 to 2023, only those occurring between January 1, 2020, and December 31, 2023, have been included

10, 2020, blogger and journalist Diantara Putra Sumedi from Kalimantan was sentenced to three months and 15 days after publishing a piece online about a land dispute between a palm oil company and the indigenous Dayak community considered to be inflammatory.⁸³

Wahyu Dwi Nugroho faced charges under Indonesia's Information and Electronic Transactions (ITE) Law for a TikTok video he posted in mid-2022 regarding shopping at stalls near the influential Majelis Taklim Al Busyro neighbourhood.

The Majelis Taklim holds significant influence in West Java and neighbouring areas. Wahyu's legal defence was provided by the Keadilan Bogor Raya Legal Aid Institute, with support from PAKU ITE, a collective of ITE Law victims formed by SAFEnNet. In a concerning turn of events, Wahyu, who had been detained since March 2023, was released on the evening of Aug. 11, 2023, following a scheduled verdict hearing at the South Jakarta District Court on Aug. 10, 2023. Surprisingly, he was sentenced to 5 months in jail. This outcome has raised serious questions about justice in his case. Wahyu's situation highlights the misuse of Article 28 (2) of the Indonesian ITE Law, which deals with "hate speech." It reveals how this law's flexibility is exploited to address a wide range of online disputes without considering power imbalances. This climate instils fear and discouragement among those wanting to express their opinions, particularly as Indonesia approaches the February 2024 election. Wahyu's case and the misuse of the ITE Law emphasise the urgent need to protect justice and democracy in Indonesia. Addressing these issues through comprehensive legal reforms will not only rectify current injustices but also strengthen the democratic principles essential for the nation's progress.⁸⁴

This article also used to stifle environmental activist expression. Daniel Tangkilisan, an environmental activist in Karimunjawa, was sentenced to 7 months in prison and fined 5 million rupiah due to the violation of 28 (2) article. Daniel is a prominent member of the Karimunjawa Struggle Movement, which fights against the illegal intensive shrimp farming practices. An affiliation of illegal intensive shrimp farmers filed a lawsuit against Daniel, after he commented on his own personal Facebook account, using the term "shrimp brain community" (or birdbrain) as an idiom to criticise the supporters of illegal intensive shrimp farming. (<https://safenet.or.id/2024/04/free-daniel-from-all-unjust-accustaions/>)

The foregoing cases make up a fraction of all instances of government overreach in limiting online speech, particularly on the basis of the ITE Law. From February to April 2021, the Criminal Investigation Bureau of the National Police issued content removal warnings against 200 social media accounts for allegedly engaging in hate speech, in contravention to Article 28(2), as part of its newly invented Virtual Police Program.⁸⁵ Created in February 2021, it had the power to warn netizens about the illegality of their posts.⁸⁶ As of March 2023, Indonesia reportedly plans to introduce new legislation tightening control over social media platforms and would allow the government to make “urgent” requests for content to be removed within four hours.⁸⁷

In 2022, pursuant to the stipulation of MR5, several major online service providers including Google, Twitter and META registered themselves with KOMINFO to avoid being blocked in the country.⁸⁸ As a result of such registration, these platforms must now comply with the government’s stringent content moderation guidelines, take down any

prohibited content identified, and provide the government access to their systems and user data stored thereon. A number of platforms who failed to comply with this registration requirement before the set deadline of July 24 were subsequently blocked; among the list were Yahoo and PayPal.⁸⁹ In August, KOMINFO stated that registered platforms could still be subject to blocking if they fail to moderate content as mandated.⁹⁰ KOMINFO representatives have since denied that MR5 poses substantial online expression and privacy risks, maintaining that it is rather necessary to enhance cybersecurity in the country.⁹¹

During the 2024 presidential election, there are also some indications that this regulation has been misused. Some posts that criticised Prabowo Subianto and Gibran Rakabuming Raka had been requested to be taken down by KOMINFO. Prabowo and Gibran is the presidential and vice presidential candidate supported by the current president, Joko Widodo and the Ministry of Communication and Informatics, Budi Arie Setiadi.

“

The three-part test has not been effectively incorporated into the legal framework of Ministerial Regulation 5, thereby opening up avenues for the infringement of freedom of expression in Indonesia. It imposes unrealistically short time frames for content removal, and would likely result in over-censorship by many digital platforms and services.

- Alia Yofra Karunian, Member of PurpleCode Collective

State Surveillance to Stifle Dissent

The government supposedly employs surveillance technologies to stifle online freedoms. The government is under suspicion of procuring spyware manufactured by Cytrox to conduct surveillance on journalists and activists,⁹² as well as utilising Circles technology.⁹³

PEGASUS TO SCARE PEOPLE INTO SILENCE

According to a disquieting report published by IndonesiaLeaks in June 2023, the insidious Pegasus spyware has been active in Indonesia since 2018, targeting a wide range of individuals, including activists, investigative journalists, media outlets, and politicians.⁹⁴

This highly intrusive tool, created by the Israeli company NSO Group, operates without the device owner's involvement and has been licenced to governments and law enforcement agencies worldwide. Its primary objective is to stealthily collect information from a compromised device and send it to a third party without the owner's knowledge or consent.⁹⁵ The programme shockingly infiltrated Indonesia via international shipment.⁹⁶ The use of spyware constitutes one of the most egregious invasions of privacy, as it monitors the most intimate mobile device activities. Regrettably, authoritarian regimes around the world have adopted Pegasus as a tool for monitoring and silencing human rights defenders, activists, and journalists who venture to expose corruption and abuses of power. It is crucial to recognise that certain forms of expression, which may not legitimately fall under the designation of terrorist activities or within the boundaries of terrorism definitions, are unjustly deemed illegal.⁹⁷

Pegasus compromises the privacy of all types of personal information, including online and offline communications. This permits governments and affiliated entities to intercept sensitive information, exposing individuals to harassment, intimidation, and potential threats to their safety. Dangerously severe consequences await those who venture to disagree, discouraging many from engaging in political activities and compelling them to self-censorship.⁹⁸

Unfortunately, since the release of the Indonesia Leaks report, there have been no discernible efforts from the government to publicly address the concerns raised regarding the acquisition practices related to Pegasus. While the report does include a statement from Indonesian Police (POLRI) asserting that they do not utilise Pegasus, it is noteworthy that they do not dispute the accuracy of the zero-click acquisition method mentioned in the report. The Indonesian Corruption Watch submitted a public information request on Oct. 7, 2023 regarding this issue, and according to regulations, law enforcement is required to respond within 14 days of receiving such requests. As of the end of 2023, there has been no response from the police.⁹⁹ It appears that the

acquisition practices detailed in the report may extend beyond Pegasus, as per information gathered from Indonesia Leaks, which could encompass various software or tools.¹⁰⁰

Furthermore, the investigation revealed a significant lead involving a company named PT Mandala Wangi Kreasindo, which

had procured intelligence-related software from a subsidiary of NSO Group known as Q Cyber Technologies. This suggests a third-party connection in the acquisition process. Additionally, when examining the acquisition made by Polda Metro Jaya, a branch of Polri, during the years 2017-2018, it was facilitated through a private company called PT Radika Karya Principal, with a clear link to zero-click technology, strongly indicative of Pegasus. This aligns with the prevailing understanding that Pegasus is the foremost and most advanced tool globally for implementing spyware via the zero-click method, as repeatedly emphasised in reports by various international agencies. In essence, it appears that despite utilising third-party intermediaries, these tools continue to find their way into Indonesia.¹⁰¹



#People Power | Crucial Intervention:

The ASEAN Regional Coalition to #StopDigitalDictatorship Call to End Pegasus Spyware Abuses¹⁰²

The ASEAN Regional Coalition to #StopDigitalDictatorship stands united in solidarity with activists and victims affected by the invasive Pegasus spyware, strongly urging the Indonesian government to promptly cease and prohibit the utilisation of targeted digital surveillance technologies. This egregious practice infringes upon fundamental rights and constitutes a grave violation of universally-protected freedoms, including the rights to freedom of expression, access to information, privacy, peaceful assembly, and association. The resultant chilling effect on civil societies and the broader civic space necessitates immediate action.

The coalition calls on the Indonesian government to adhere to international human rights standards concerning privacy, as articulated in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Additionally, the government is urged to respect the rights to freedom of expression and information, enshrined in Article 19 of the UDHR and ICCPR.

Denouncing the systemic failure to meet international human rights obligations, the ASEAN Regional Coalition criticises the violation of people's rights to freedom of expression and privacy, guaranteed by national laws. Articles 28, 28E, and 28F of the 1945 Constitution safeguard the right to freedom of expression, while Article 28G protects the right to privacy. The recently enacted Personal Data Protection (PDP) Act of 2022 further solidifies

privacy and data protection rights. The coalition emphasises that mass surveillance contradicts the concept of privacy and infringes upon fundamental rights protected by national and international law.

The ASEAN Regional Coalition to #StopDigitalDictatorship issues a compelling call to the Indonesian government to implement an immediate ban on spyware technology in collaboration with civil society and the private sector to prevent human rights abuses. The coalition also urges reaffirmations of protections for activists and human rights defenders, recognizing their legitimate work and safeguarding freedom of expression and civic space.

Furthermore, the coalition calls for the establishment of judicial and non-judicial grievance mechanisms for victims to seek remedy, with due process and judicial oversight integral to the surveillance spyware regime. It emphasises the need to ensure that the use of surveillance technology aligns with domestic laws and international human rights standards of legality, necessity, proportionality, and legitimacy. The coalition stresses the importance of making information regarding the acquisition of surveillance technology accessible to the public, fostering open discussions necessary for a democratic society. The coalition further calls upon the international community to enforce a strict moratorium on the export, sale, transfer, and use of highly intrusive spyware tools such as Pegasus until robust regulations guarantee compliance with international human rights standards.



Cyber-attacks on HRDs and Activists Continue to Erode Democracy

Much like other Southeast Asian countries, Indonesia is not a safe place for HRDs and activists to express their views online. A range of cyber torture techniques are employed, the most prominent being intimidation, humiliation, slander, and doxxing.¹⁰³ As human rights activism increasingly became digital in the wake of the COVID-19 pandemic, the methods of attacks diversified to include Zoom-bombing and SMS phishing. Out of 147 digital attacks SAFEnet recorded throughout 2020, 66 or 44.90% targeted critical voices such as journalists, activists, university students, and civil society organisations.¹⁰⁴ In 2021, SAFEnet reported 193 incidents of digital attack, with activists being targeted in 50 of them, civil society in 10 and media workers in 25.¹⁰⁵ Another data, however, shows that the total number of attacks against HRDs in that same year stands at 120.¹⁰⁶ In 2022, there were at least 97 cases of criminalisation related to expression in the digital realm, with 16 involving activists and 11 involving student activists. They both rank among the top 5 most victimised groups of 2022.¹⁰⁷ Data for 2023 SAFEnet report has not yet been released.

In May 2021, some 50 former members of KPK who had been discharged for having allegedly failed the National Knowledge Examination—a test designed to gauge one’s proficiency in Indonesia’s state ideology—reported being doxxed, Zoom bombed with pornographic materials and having their email accounts hacked by anonymous persons.¹⁰⁸ The events persisted through September, targeting different former members and individuals who protested the discharge.¹⁰⁹

In another case, independent media outlet Project Multatuli, became a victim of digital attacks after launching an online campaign with the hashtag #PercumaLaporPolisi (lit. #NoUseReportingto-

Police) in relation to law enforcement’s failure to handle a rape case involving three minors in East Luwu, South Sulawesi. Project Multatuli’s website, on which a piece on the case was also published, was subjected to a series of DDoS attacks and became inaccessible for a period of time.¹¹⁰

Moreover, state authorities regularly block access to websites and online news outlets perceived to be critical of the administration.¹¹¹ Among those that have been blocked are information-sharing blogs such as Reddit and websites focused on political content, gaming, alcohol and drugs, gambling and online dating.¹¹² In July 2022, Indonesia implemented additional restrictions by blocking access to various online platforms, including the search engine website Yahoo, payments from PayPal, and several gaming websites. These actions were taken due to the failure of these platforms to comply with licensing regulations imposed by authorities.¹¹³ In 2023, Indonesia blocked 14 websites comprising 16 links in the category of Political Criticism and Terrorism and Militants. More than half of the blocking indicated HTTP blocking only (51.6%) as opposed to DNS tampering only (32.3%) or both DNS tampering and HTTP blocking (16.1%).¹¹⁴ Blocking is rarely, if ever, done with transparency as to its justification and duration. There has also been a proliferation of state-sponsored “buzzers” on social media platforms who are hired by the government to promote state policies or spread disinformation to manipulate public opinion on certain sensitive issues, oftentimes by using doxxing or harassment techniques. Buzzers receive between IDR 1 and 50 million (\$66–3,344) for their work, and are largely employed on a contractual basis.¹¹⁵ One buzzer team leader interviewed by Reuters revealed that he was able to control more than 250 accounts spread across Facebook, Instagram, Twitter, and other major platforms during one operation, each with a false persona.¹¹⁶ Buzzer support was notably widespread during the 2019 crackdown on a series of protests

in Papua and ahead of the general election.¹¹⁷ Political cyber troops are known to be a common and highly effective tactic to stifle online expression.¹¹⁸ However, their impact extends beyond domestic affairs. In December 2023, their actions took on a new dimension with the resurgence of fake UN accounts. These impostor accounts played a significant role in exacerbating anti-Rohingya sentiment, posting anti-Rohingya messages and further complicating advocacy efforts for freedom of expression in Indonesia. This highlights the urgent need for safeguards against online misinformation and manipulation.¹¹⁹

Online Content Manipulation & Restrictions

Government Requests to Remove or Restrict Content or Accounts

The Indonesian authorities regularly issue requests to websites and social media platforms to remove information or content on their platforms. In 2020, Meta received 772 restriction requests in total and restricted access to 760 items on grounds of alleged violations of local laws. In 2021, it received 1009 requests for both platforms (Facebook and Instagram) and restricted access to 4,011 items in total. The first half of 2022 saw a decrease, with 1,475 requests and 1,458 items being restricted on the two social media websites. In the second half of 2022, 2,590 contents were restricted. Finally, the first half of 2023 consisted of 5,240 requests.¹²⁰

Google reported to have received 66 requests in 2020 across its platforms and had a compliance rate of 24.4% in the first half of the year and 60.9% in the second half. It reported 426 requests in 2021 and notably complied with 88.6% of them in the second half of the year. In 2022, Google had 309 requests and a compliance rate of 56.8%. For 2023, 224 requests were made.¹²¹

In 2020, **Twitter** received 291 requests, and in 2021, it reported 269 requests. Its latest reports show a climb in compliance rate similar to that of Google, from 28.1% in 2020 to more than 60% in 2021. The transparency report from Twitter only covers data up to the end of 2021 for all countries. From 2020 to 2022, TikTok received few requests to remove and/or restrict content due to local law violations. For the first half of 2023, 225 requests were made.¹²³

TECH COMPANIES COMPLICIT OF DIGITAL DICTATORSHIP: THE CASE OF TELEGRAM IN INDONESIA



Regarding Telegram specifically, the government imposed a temporary prohibition on the messaging application in 2018 on the grounds that it facilitated communication between terrorists. Following Telegram's commitment to enhance content moderation and establish a representative office in Indonesia, the prohibition was lifted. According to a report by Nava Nuraniyah (2017), the underlying rationale for the blockade was not to suppress extremism, as the statement asserts. On July 17, three days subsequent to the prohibition, Durov, the CEO of Telegram, issued a statement wherein he admitted to his delayed reaction to the government's appeals to obstruct certain extremist channels and pledged to enhance collaboration with the government by means of establishing a "direct line of communication." However, it was not sufficient. To further compel the lifting of the prohibition, the government has now mandated that Telegram establish a local office in Indonesia, akin to the operations of Google, Yahoo, and Facebook. The level of concession that Telegram will offer is yet to be determined. Eliminating Telegram access is, at best, a strategic manoeuvre employed to align the operations of tech behemoths with governmental regulations.¹²⁴



PANDEMIC POLITICS: COVID-19 IMPACT ON ONLINE ACTIVITIES

The COVID-19 pandemic has allowed authorities to constrict civic space in the country and freedom of expression was limited excessively. Social media users who criticised the government's handling of COVID-19 have been charged under ITE Law for allegedly spreading disinformation about the COVID-19 pandemic. In the two-year window between January 2020 and 2022, authorities have opened investigation into and prosecuted 767 pandemic-related disinformation cases.¹²⁵ Police order No. ST/1100/IV/HUK.7.1.2020 came into force in April 2020, giving police emergency powers to conduct "cyber patrols" and monitor online discussions around COVID-19, the government's handling of it, and any other information surrounding this topic.¹²⁶

The pandemic allowed authorities to limit freedom of speech excessively in the country. In 2020, a university professor said that hackers released images of him and a woman they claimed to be his mistress on his Twitter page after he criticised the government's handling of the COVID-19 pandemic.¹²⁷ Several other organisations alleged that hackers erased content from their websites, while media outlets and civil society organisations, including Tempo, Tirto.id, and the Centre for Indonesia's Strategic Development Initiatives (CISDI), were hacked after posting articles criticising the pandemic management.¹²⁸ In another Article 28(2) case, Wira Pratama, a resident of Riau Islands off the coast of Sumatra, was prosecuted for uploading on his personal Facebook account a meme of President

Widodo with the caption “[w]e will be watching if you corrupt the COVID-19 fund”. On April 8, 2020, Pratama was arrested for spreading hatred towards and insulting the President.¹²⁹

The government has also routinely required platforms and content moderators to remove negative content related to COVID-19. For instance, in 2021, Facebook restricted access to 2,483 items, purported to be false COVID-19-related claims.¹³⁰ The MCIT claimed to have identified 2,442 hoaxes and misinformation spread across various social media platforms from January 2020 through

November 2021.¹³¹ Some of these cases are still under investigation while the remaining majority ended in access blocking by the government, under either account suspension or content takedown. It is unclear what criteria were used to classify content as a hoax or misinformation and whether procedural standards were complied with in responding to these findings. There are also vast inconsistencies in the numbers disclosed by different officials, rendering difficult any attempt to have an accurate estimate of the actual case count.¹³²



INTERSECTIONAL GENDER ANALYSIS: ONLINE GENDER BASED VIOLENCE IN INDONESIA

When addressing issues related to Online Gender Based Violence, hereinafter referred to as “Kekerasan Berbasis Gender Online” in Indonesian, it is crucial to understand the underlying dynamics of gender power relations. Both the digital space and offline space are important democratic and civil domains that should be accessible and safe for all members of societies including women, children and LGBTIQ+.

Current reports highlight that women are the primary group facing technology-facilitated gender-based violence. Additionally, minority communities, particularly the LGBTIQ+ population, are targeted due to their identities. Strikingly, Indonesia lacks legal protection for LGBTIQ+ individuals against hate crimes and discrimination, leaving them exposed to online abuse, including “cyber-homophobia” based on sexual orientation.¹³³ State authorities contribute to the issue by

spreading online homophobic and transphobic narratives, escalating to online violence. Instances include the Indonesian Air Force’s discriminatory policies and a former minister justifying violence against LGBTIQ+ individuals based on religion. Media outlets exacerbate the problem by using stigmatising language, blaming the LGBTIQ+ community for natural disasters. This pervasive online hostility, fueled by state authorities and media, underscores the urgent need for comprehensive measures to address technology-facilitated GBV, recognising the unique challenges faced by women and the LGBTIQ+ community in Indonesia.¹³⁴

Spotlight on the OGBV and judicial harassment faced by Veronica Koman

However, within Indonesia’s complex digital landscape, marginalised groups, including women

human rights defenders, grapple with formidable challenges, encountering instances of OGBV. For example, consider Veronica Koman, a woman human rights defender advocating for the West Papuan indigenous peoples.¹³⁵ Since 2019, she faces OGBV, experiencing death threats, rape threats, racist and misogynistic abuse via social media. She has been labelled a traitor due to her tweets about the situation in Papua and a crackdown on pro-Papuan independence activists in Surabaya, East Java, sparking weeks of protests.¹³⁶

Additionally, Veronica Koman faces charges in Indonesia, including alleged “incitement,” “spreading fake news,” “displaying race-based hatred,”¹³⁷ and “disseminating information aimed at inflicting ethnic hatred.” The threats extend to Koman’s family, underscoring the intersectionality of being a woman human rights defender facing risks that also extend to her family. In December 2021, the UN Special Rapporteur on the situation of human rights defenders, Mary Lawlor, condemned Indonesia to immediately cease threats, intimidation, and reprisals against human rights defender Veronica Koman and her family.¹³⁸ Currently, Veronica Koman is in self-imposed exile in Australia due to considerable risks to her security in Indonesia.¹³⁹

Lack of support and access to remedy for survivors of OGBV cases

Despite these challenges, a comprehensive analysis gap persists among public interest lawyers and peer assistants providing support to justice seekers in this context. One significant issue that needs to be addressed is the imbalance between the availability of institutions and communities dedicated to handling OGBV cases and the increasing number of OGBV cases year by year.¹⁴⁰

The Task Force KBGO, initiated by PurpleCode

Collective, is dedicated to providing assistance for victims through three pillars: legal aid, technological aid, and psychological aid. In 2022, out of the 98 complaints received by Task Force KBGO, 82 of them were submitted directly by victims, while the remaining 16 complaints were filed by companions such as family members or friends. The majority of complaints, both from victims and companions, came from individuals in the 21-25 age group. The highest number and percentage of complaints were from 21-year-olds, making up 13.27% of the total complaints. Following closely were 25-year-old complainants, accounting for 12.24% of the total. The third-highest number of complaints came from 24-year-olds, with 10 complaints (10.20%). On the other hand, individuals aged 28, 30, 37, 38, and 49 each made up only 1.02% of the total complaints. Among the 98 complainants, there were two individuals for whom Task Force OGBV couldn’t ascertain their identities. These two victims were referred to Task Force KBGO by the National Human Rights Commission, Komnas Perempuan.¹⁴¹

Young people are more at risk of the OGBV

According to the 2022 Indonesian Internet Profile released by the Indonesian Internet Service Providers Association (APJII), the largest group of internet users falls within the 19-34 age bracket. This data supports the dominance of the 21-25 age range among complainants. It suggests that individuals in this age group have more extensive internet access, making it relatively easier for them to find Task Force KBGO and file complaints. However, this doesn’t necessarily imply that other age groups are less susceptible to experiencing OGBV. It may simply be due to variations in internet access among different age groups, which could be addressed by ensuring

broader coverage.¹⁴²

Among the 80 complaints identified by Task Force OGBV, the age range of the victims spanned from 14 to 45 years. Notably, victims aged 21 years old were the most frequent, comprising 13.41% of the total complaints. Additionally, there were 10 victims (12.20%) aged 25 years, eight victims (9.76%) at 24 years, and six victims (7.32%) aged 17 years. It's worth highlighting that two age groups, 14 and 17 years old, fall within the children's category according to the Convention on the Rights of the Child, which defines children as those under 18 years old. This underscores the gravity of OGBV affecting children, with potentially more severe and lasting impacts.¹⁴³

The different forms of OGBV in Indonesia

Furthermore OGBV encompasses various forms of online violence, includes doxing, extortion, impersonation, psychological violence, verbal abuse, photo and video manipulation, content coercion, unauthorised content storage, non-consensual recording and dissemination of intimate images (NCII), online stalking, outing, forced abortion, hacking, sextortion, tech-enabled surveillance, and trolling. Often, when victims or their companions approach Task Force KBGO, they may not be aware of the specific type of KBGO they are experiencing. What unites them is the presence of threats and violence.

According to Task Force KBGO, sextortion, a form of violence involving sexual threats, constitutes the majority of OGBV cases handled in 2022. Task Force KBGO dealt with 64.29% of the 98 reported cases. This number is significant and alarming, surpassing more than half of all OGBV cases that Task Force OGBV addressed. Sextortion cases sometimes overlap with other forms of OGBV,

such as NCII (Non-Consensual Dissemination of Intimate Images), extortion, and doxing.

NCII, the second most common type, accounted for 26.53% of cases. NCII involves the act of perpetrators distributing intimate photos or videos of victims without their consent (PurpleCode Collective, 2020). These media may have been created consensually between the victim and the perpetrator or solely by the victim and then shared with the perpetrator. For Task Force KBGO, this highlights the importance of a layered approach to consent. Just because someone consents to creating or sending a photo/video does not imply consent to its dissemination. The act of creating/sending and the act of sharing are distinct actions, and consent should be obtained for each of these actions separately.

It's important to note that consent follows these principles:

- Layered (across actions, individuals, times, places, and platforms).
- Can be withdrawn at any time and is not perpetual.
- Clearly informed.
- Silence does not equate to consent.

Following NCII, the subsequent breakdown of OGBV cases is as follows: recording without consent, trolling, storing recordings without consent, and extortion, each accounting for 16.33%, 11.22%, 10.20%, and 10.20%, respectively. Next in line are doxing at 4.08%, verbal violence at 2.04%, content coercion at 3.06%, forced content transmission at 6.12%, online stalking at 2.04%, outing at 5.10%, and hacking at 5.10%.

The lowest percentage is attributed to impersonation, psychological violence, photo and video manipulation, unauthorised content storage, forced abortion, and tech-enabled surveillance, each at 1.02%.¹⁴⁴

How to address cases of OGBV?

OGBV in Indonesia and anywhere often involves multiple types, making cases intricate. Relevant solutions must be tailored to each OGBV type experienced by victims. Hence, it is necessary to frequently engage with various individuals and organisations to inquire and collaborate on OGBV cases. In handling OGBV cases, we need to acknowledge that it cannot be a one-size-fits-all solution.¹⁴⁵

Digital Darkness: Unmasking the Ominous Surge of Online Hate Campaigns Against Rohingya Refugees in Indonesia

What happened?

Amid Indonesia's digital repression, a dire situation has emerged with the plight of Rohingya refugees seeking shelter in Aceh, including areas like Sabang, Pidie, and Bireuen. Drawing parallels to the lead-up to the 2017 Rohingya genocide in Rakhine State, online disinformation and hate speech comments targeted at Rohingya refugees in Indonesia are now contributing to an unsafe environment.¹⁴⁶ This is evident through the systemic dissemination of content depicting Rohingya refugees in Indonesia in a negative light, for example, portraying them as disrespectful to their host country, or accusing them of wasting food aid.¹⁴⁷ Destructive narratives persist, stigmatising Rohingya individuals as 'illegal' immigrants and portraying them as

perceived threats to local customs, regulations, and norms.¹⁴⁸ The Rohingya people are subjected to malicious hate speech and face various forms of violence, including persecution, deprivation of citizenship, and genocide in their homeland, Myanmar. This not only exacerbates their physical suffering but also inflicts profound psychological scars, adding another layer of difficulty to their struggle for support and the acknowledgement of their basic human rights.¹⁴⁹

Further, these dehumanising narratives are purposefully crafted to sow anxiety and fear among the local Acehnese population, cultivating the unfounded belief that welcoming Rohingya refugees would overwhelm and jeopardise Acehnese resources. It is crucial to highlight that the recorded Rohingya population in Aceh stands at a mere 1,700 individuals, constituting a negligible fraction compared to the 5.4 million Acehnese residents.¹⁵⁰

Social Media Onslaught: Unveiling the Shocking Hostility Towards Rohingya

The evidence underscores a disturbing reality: The UN's official Instagram account, @UNinIndonesia, has been inundated with 17,380 comments since November 21, 2023, specifically targeting four posts related to Rohingya. The UN's assessment revealed a staggering 91 per cent of these comments qualified as "hate comments".¹⁵¹ Moreover, the UNHCR itself has also become the target of what it has called an "orchestrated" disinformation campaign on social media platforms such as TikTok and Instagram, referring to the emergence of social media accounts spreading anti-Rohingya rhetoric, all while falsely claiming to be UN-affiliated.¹⁵² TikTok made a statement that accounts impersonating UNHCR Indonesia

“will be removed;” in response to a request for comment made by This Week in Asia, while Meta did not immediately respond.¹⁵³

In the absence of intervention, the unchecked proliferation of disinformation poses a grave risk, potentially culminating in heightened waves of targeted attacks – and even atrocities – against Rohingya refugees in Indonesia and the broader South and Southeast Asian region. The systematic dissemination of online hate speech targeting the Rohingya has historically served as a catalyst for previous instances of targeted assaults on this vulnerable community. It is indisputable that the inadequacy of regulatory frameworks in managing this hostile online environment significantly contributed to the tragic events of the 2017 genocide against the Rohingya, compelling their forced displacement to neighbouring countries within Myanmar.¹⁵⁴

4.3 Access to Effective Remedy

The Indonesian Constitution contains general references to the right of individuals to access courts and administrative bodies to seek damages. In practice, however, this constitutional guarantee is often impeded by corruption and political influence within the system. Cyber laws are also not equipped with provisions on access to an effective remedy in case of a breach, nor do these laws set up procedural safeguards and an independent mechanism to oversee their implementation. Thus, individuals or entities who suffer the consequences of a misinterpretation or misapplication of those cyber laws are all but deprived of their right to obtain redress.¹⁵⁵

Due to the limited recognition of Strategic Lawsuits Against Public Participation (SLAPP) within the Indonesian legal framework, coupled with the absence of anti-SLAPP jurisprudence, human rights defenders (HRDs), activists, or any individual embroiled in judicial harassment cases face significant challenges. Without the option to have their cases dismissed, they are compelled to navigate through a protracted and costly judicial

process, leaving them even more vulnerable or sometimes completely incapacitated and paralysed.

Moreover, within the Indonesian legal system, crimes of libel and defamation under the Criminal Code can only be prosecuted through a complaint lodged by an injured party. Such a complaint mechanism is what is often wielded by individuals or certain groups with vested interests to target their critics. Equally problematic is Article 312 of the Criminal Code which provides that judges may assess the falsity of alleged libellous or defamatory statements only in cases where such an assessment is (1) necessary to test an accused’s assertion that he had been acting in pursuance of a general interest or self-defence or (2) the accused is a public official acting within his official powers. This formulation gravely restricts an accused’s scope of defence in court. By extension, it hinders access to an effective remedy for HRDs and activists who face charges for attempting to expose wrongdoing by authorities or private persons.¹⁵⁶

Non-Judicial Grievance Mechanisms Available, but Not Sufficient

State-based non-judicial grievance mechanisms are available; individuals can file complaints to the Indonesia National Commission on Human Rights, or *Komnas HAM*. The Commission is authorised to conduct inquiries into gross human rights violations under the 2000 Law on the Establishment of an *Ad Hoc* Human Rights Court.¹⁵⁷ Inquiries initiated by the Commission, however, do not automatically trigger a prosecution, nor does they make prosecution more likely to take place. Complaints handled by the Commission rarely amount to criminal charges, leaving high levels of impunity. This is partly due to the fact that the Attorney General's Office, who is in charge of deciding whether cases of gross human rights violations can proceed to litigation, rarely decides so.¹⁵⁸ Furthermore, politics and the backgrounds of commissioners can exacerbate this general hesitance to see complaints through. A religiously conservative commissioner, for instance, would assess a case in a manner different from someone with a background in human rights activism.¹⁵⁹ As a result, the Commission's role rarely pierces through the investigatory or advisory capacity, making it even more unlikely for digital freedoms breaches to be remedied through this avenue.¹⁶⁰

Whistleblowers Protection and Environmental Cases

Whistleblowers and activists are especially vulnerable to state-backed harassment for expressing themselves online. Indonesia does not have a comprehensive whistleblower protection regime; the 2006 Law on Witness and Victim Protection is the only piece of legislation that sets out their fundamental rights.¹⁶¹ The Law has a number of shortcomings, including that whistleblowers are merely characterised as "reporters" of suspected crimes. Thus, anyone

who discloses sensitive information related to a crime they know about, which may be done in the online space, would not enjoy special protection. In addition, the oversight body in charge of administering protection for victims and witnesses, the Witness and Victim Protection Agency (LPSK), operates in tandem with other agencies that are known for their corrupt practices and lack of independence, such as the Corruption Eradication Commission (KPK) and the National Police. Therefore, the Law's implementation is substantially hindered by lack of transparency and institutional gaps.¹⁶²

Environmental Cases

In addition, there are laws in place that prevent the filing of lawsuits against individuals who advocate for environmental rights. For instance, the 2009 Law on Environmental Protection and Management, and the 2013 Law on the Prevention and Eradication of Forest Destruction offer such protection. Furthermore, individuals who provide information about or report on environmental issues are also safeguarded by these laws. However, it's important to note that while these laws are generally seen as a response to Strategic Lawsuits Against Public Participation (SLAPP), they lack a specific definition of SLAPP and only apply to environmental cases. Consequently, they may not provide sufficient grounds for SLAPP defendants to have their cases dismissed, nor can judges rely on them to prevent legal abuses.¹⁶³

Chapter V.

Recommendations

In this chapter, we will discuss recommendations regarding the governance of the digital space in Indonesia. These recommendations are addressed to different stakeholders.

Recommendations to Governments

- 1 Decriminalise by repealing or amending the provision on defamation (Articles 142, 144, 207, 208, 310 (2), 310 (3), 311, 315, 317, 318, 320, 321 of the old Criminal Code as well as Article 27A of the Second Amendment of the ITE Law), fake news (Articles 28 and 45 A(3) of the Second Amendment of the ITE Law), religious blasphemy (Article 156a of the old Criminal Code), termination of electronic and information access (Article 40 (2b) of the Second Amendment of the ITE Law), potentially inflicting secondary victimisation to the victim of gender-based violence (Article 27 (1) of the Second Amendment of the ITE Law), as well as repealing the new Criminal Code that is scheduled to come into force on January 2, 2026, specifically on defamation (Articles 218-219 and Articles 240-241), fake news (Articles 263-264), religious blasphemy (Articles 300-305), bringing them in line with article 19 of the International Covenant on Civil and Political Rights;
- 2 Enact a stand-alone anti-SLAPP law to ensure legal protections against strategic lawsuits against public participation (SLAPP) aiming at silencing dissent, and protect individuals from judicial harassment by the state and corporations;
- 3 Repeal or substantially amend laws and regulations that unduly restrict freedom of expression, independent media, and access to information, to bring them in line with international human rights law. In particular, clarify or reform vague laws, so that they are written in ways that are comprehensible and accessible to all members of society, so that all society members are aware of their responsibilities, protections, and the consequences of not abiding. This includes notably the old Criminal Code, new Criminal Code and the Second Amendment of the ITE Law. The repeal or amendment process should include effective public consultation (in particular, taking into account historically marginalised opinions);
 - a. Clarify legal responsibility under civil and administrative law for what constitutes 'online gender-based violence (OGBV),' 'hate speech,' 'hateful conduct,' 'harassment,' 'doxxing,' and other key terms, while simultaneously upholding the right to freedom of expression and opinion. Enable people of marginalised groups (e.g. women, LGBTIQ+, disabled peoples, people marginalised based on race, Indigenous peoples, etc.) to guide and participate in the development of reasonable definitions for terms used in legislation that disproportionately affect them. Ensure that reports of online gender-based violence (OGBV) are subject to systematic and consistent investigation, and offer assistance to individuals or groups affected;
 - b. Expand any definitions of 'personal information' and/or 'private information' to protect (if not already protected) an individual's full legal name; date of birth; age; gender/legal sex; LGBTIQ+ identity; places of residence, education and work; private personal information of family members and relatives; descriptions and pictures depicting an individual's physical appearance; and screenshots of text messages or messages from other

platforms. These should be considered when investigating cases of doxxing, smear campaigns, and other instances of online violence that weaponise an individual's personal/private information against them. Ensure that reports of doxxing campaigns and other forms of violence on the digital space are subject to systematic and consistent investigation, and offer assistance to individuals or groups affected.

- 4 When punishing expression as a threat to national security under Articles 142, 144, 207, 208, 310 (2), 310 (3), 311, 315, 317, 318, 320, 321 of the old Criminal Code as well as Article 27A of the Second Amendment of the ITE Law, the government must demonstrate, with evidence, that:
 - a. the expression is intended to incite imminent violence;
 - b. it is likely to incite such violence; and
 - c. there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence, in line with the Johannesburg principles;¹
- 5 Guarantee transparency and access to information, both offline and online, particularly where such information relates to the public interest and impacts upon the individual's right to public participation, including by amending existing laws or adopting a law to enable provision of such access. Implement measures to enhance transparency in political advertising, including clear disclosure of funding sources and target audiences to promote accountability and integrity, and combat disinformation;
- 6 Ensure that any internet shutdowns or restrictions are proportionate, necessary, and comply with international human rights law, including providing transparent justification and legal oversight;
- 7 Enable HRDs, journalists, civil society members, ordinary users, lawyers and academics to safely carry out their legitimate online activities to spread awareness for human rights violations without fear or undue hindrance, obstruction, judicial harassment, and/or online harassment (e.g. OGBV and general OBV, non-consensual sharing of intimate pictures online, the spread of deep fakes, hate speech campaigns, or doxxing);
- 8 Working with responsible MPs and with tech companies, enforce social media policies to prevent harmful effects of doxxing, while considering applicable regulations in Indonesia. Establish an independent committee, if not already in place, to ensure compliance with these regulations, with a particular focus on moderating or removing illicit content.
- 9 Repeal or amend all laws and regulations that establish a licensing regime for the print and online media, replacing them with a system of self-regulation;
- 10 Cease the targeting and criminalisation of legitimate online speech by opposition activists, journalists, HRDs, and other dissenting voices solely in the exercise of their rights to free expression online, through the abuse of laws and administrative regulations;
- 11 Prevent acts of harassment and intimidation against, the placement of arbitrary restrictions on, or arrests of journalists, activists and human rights defenders who merely criticise public officials or government policies;

1. ARTICLE 19, *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, (November 1996), available at: <https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

- 12 Recognise online and technology facilitated OGBV as a human rights violation and include it in laws to criminalise and prohibit all forms of violence in digital contexts. Enhance the capabilities of law enforcement agencies to effectively investigate and prosecute such crimes;
- 13 Strengthen collaboration with the technology industry, feminist organisations, civil society, and national and regional human rights bodies to bolster measures and policies aimed at promptly and effectively providing remedies to victims of OGBV;
- 14 Implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place to regulate such practices. In cases where such technologies have been deployed, ensure both targeted individuals and non-targeted individuals whose data was accessed as a result of someone else's surveillance are notified, implement independent oversight, and ensure targets have access to meaningful legal remedies;
- 15 End all legal proceedings against individuals facing investigation, charges or prosecution initiated by state authorities for engaging in legitimate activities protected by international human rights law or for addressing violations. Cease all violence against independent media and journalists allowing them to freely report on the emerging situation in the country and stop all efforts to restrict independent information from reaching people;
- 16 Legally recognise human rights defenders and provide effective protection to journalists, HRDs and other civil society actors who are subjected to intimidation and attacks owing to their professional activities;
- 17 Ensure that all measures restricting human rights that may be taken in response to mass-destabilising events, including public health emergencies such as a global pandemic, are lawful, necessary, proportionate and non-discriminatory. Review the measures taken in response to the pandemic in order to ensure that a clear and sufficient legal framework exists for the response to any future pandemic, and take a cautious, progressive approach to emergency measures, adopting those that require derogation only as a last resort when strictly required because other, less restrictive options prove inadequate. This includes notably Section 5 of the 1959 State of Emergency Law, Section 11 of the 2020 COVID-19 Law, Ministerial Regulation Number 5/2020 on Private Electronic System Operators (MR 5/2020), Satgas Penanganan COVID-19 Task Force (March 2020), and PeduliLindungi tracking device (April 2020);
- 18 Take immediate steps to ensure and protect the full independence and impartiality of the judiciary and guarantee that it is free to operate without pressure and interference from the executive;
- 19 Facilitate the participation, leadership, and engagement of a diverse range of people of marginalised communities in government. Create task forces to take proactive initiatives to safeguard marginalised communities (e.g. women, LGBTIQ+, and people marginalised based on ethnicity) from specific forms of abuse, (e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn), doxxing, hate speech, and overall gender-based violence.
- 20 Carry out routine assessments of the state of digital rights under the jurisdiction. Facilitate the creation of task forces, consisting of individuals trained in the safeguarding of digital rights, to investigate these affairs.

- 21 Set up accessible and appropriate, judicial and non-judicial grievance mechanisms; Provide, among the remedies, fair treatment, just compensation or satisfaction, and the establishment of sufficient grounds to avoid its repetition. Also, implement an evaluation system that regularly screens the existing mechanisms.

Recommendations to Members of Parliament

- 1 Propose amendments to the old Criminal Code and the Second Amendment of the ITE Law as well as repeal the new Criminal Code to address all shortcomings in line with international human rights standards such as UDHR and the ICCPR; and gather consensus among other MPs to ensure these amendments are adopted into the text of the law;
- 2 Hold the government accountable by ensuring that the steps taken by government bodies and agencies in the legal framework are evaluated and analysed on an individual as well as regular basis, applied only in cases where there is a risk of serious harm and cover both the enterprises in the public and private sector without discrimination, particularly when such a step could result in the violation of rights of individuals affected;
- 3 Build discussion and debate around digital rights with specific attention paid to the Indonesia context as well as good practices adopted regionally and internationally, with the general public actively involved in providing the grassroots perspective;
- 4 Adopt and enforce national laws to address and punish all forms of gender based-violence, including in the digital space. Legal and policy measures to eradicate OGBV should be framed within the broader framework of human rights that addresses the structural discrimination, violence and inequalities that women and other communities marginalised based on gender (e.g. the LGBTIQ+ community) face. Policies should also highlight specific forms of abuse that people marginalised based on gender often face online (e.g. doxxing, non-consensual sharing of intimate pictures online, the spread of deep fakes);
- 5 Adopt specific laws and measures to prohibit new emerging forms of OGBV, as well as specialised mechanisms with trained and skilled personnel to confront and eliminate OGBV;
- 6 Organise and take responsibility for task forces that will take proactive initiatives to safeguard marginalised communities (e.g. women, LGBTIQ+, people marginalised based on ethnicity) against specific forms of abuse (e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn), doxxing, hate speech, and overall gender-based violence.
- 7 Ensure that the opposition parties are allowed to fully participate in drafting and passing legislation to enable them to fully represent their constituents.

Recommendations to Tech Companies

- 1 Ensure the companies' terms of services and policies are uniform and in compliance with international standards on freedom of expression, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological, and societal developments, in line with the obligation to respect human rights under the UNGPs;
- 2 Drop the for-profit business model that revolves around overcollection of data. Such business models are being utilised by the government and are violating data rights.
- 3 Adopt the Global Network Initiative Principles on Freedom of Expression and Privacy;
- 4 Clearly and completely explain in guidelines, community standards, and terms of services what speech is not permissible, what aims restrictions serve, and how content is assessed for violations;
 - a. Ensure tech companies recognise gendered hate speech as hate speech,
 - b. Ensure profanities and slang in Indonesian local languages directed against human rights defenders are considered hate speech, including less common words or phrases which convey the same threat of serious harm as "kill", "murder" or "rape".
- 5 Ensure the integrity of services by taking proactive steps to counteract manipulative tactics utilised in the dissemination of disinformation, including the creation of fake accounts, amplification through bots, impersonation, and the proliferation of harmful deep fakes.
- 6 Prioritise prediction of, preparation for, as well as protection against digital dictatorship and online-based violence when launching, revolutionising, or reforming products, services, and initiatives. The guidelines of the Center for Countering Digital Hate (CCDH) 'STAR Framework' should be urgently considered, which include: safety by design; transparency in algorithms, rules enforcement, and economics; accountability systems implementation; and corporate responsibility.² In addition, these predictive, preparative, and protective factors must take into account and implement the input of marginalised communities (e.g. LGBTIQ+ peoples, women, and those marginalised based on race) who often become targets of online violence that is often unregulated or even perpetuated by existing systems;
- 7 Products, services, and initiatives must have consumer safety in mind from the very beginning of conception. This means that product, service, and initiative developers, as well as high-level executives, must all take all possible measures to ensure that their products are safe, by design for all users, including marginalised communities (e.g. including LGBTIQ+ peoples, women, and those marginalised based on ethnicity). Not only does far-sighted consideration ensure user safety and the safeguarding of human rights, but it will also increase the longevity of these products, services, and initiatives in a rapidly changing economy where people are becoming increasingly aware and adamant about the protection of their human rights. Ensuring safety by design includes the practice of performing thorough risk assessments, and educating

2. CCDH, *PUBLIC SUPPORT FOR SOCIAL MEDIA REFORM: Assessing CCDH's STAR Framework for social media regulation*, (16 August 2023), available at: <https://counterhate.com/research/public-support-for-social-media-reform-star/>; The following recommendations will elaborate on this.

developers as well as executives to recognise their responsibilities to uphold human rights standards during the development as well as execution processes;

8 Promote transparency. CCDH specifically highlights the need for transparency in “algorithms; rules enforcement; and economics, specifically related to advertising.”³ Though transparency is more of a ‘preparative’ factor rather than a ‘preventive’ one, it will make civic engagement and corporate accountability much more effective, ultimately amounting to increased ‘prevention’ efficacy;

a. Transparency in algorithmic development, for example, is essential; though algorithms are not responsible humans, they were created by responsible humans. This same logic can be applied to company regulation development processes, as well as advertising strategy. For example, if company regulations were formulated in a way that disproportionately excludes marginalised voices (e.g. without any adopted input from a diverse range of people of intersectional identities, such as women, LGBTIQ+ people, disabled people, or people marginalised based on ethnicity), those regulations are more likely to cause or perpetuate human rights violations. Companies should implement measures to enhance transparency in advertising, including clear disclosure of funding sources and target audiences to promote accountability and integrity, and combat disinformation;

9 Transparency goes hand-in-hand with effective corporate regulatory and accountability systems. The people who run and work for tech companies, like consumers, are humans, who must be proportionately held

accountable for their actions if they intend to create products, services, and initiatives for consumption by civil society. Companies and their stakeholders (particularly senior executives) must recognise they hold a lot of economic, political, and social power by virtue of being in their positions, and thus naturally hold more responsibility than the average consumer. This means that though consumers have their own responsibilities, companies cannot put responsibility disproportionately on the consumer to regulate their own use of the companies’ products, services, and initiatives, if these companies genuinely intend to safeguard human rights. Thus, companies must implement regulatory systems that put people above profit, in order to allow themselves to be held accountable, and in order to facilitate their self-regulation;

10 Enable people of marginalised groups (e.g. women, girls, LGBTIQ+ people, disabled people, people marginalised based on ethnicity), to participate and lead in the technology sector to guide the design, implementation, and use of safe and secure digital tools and platforms;

11 Commit to eradicating OGBV and allocate resources to information and education campaigns aimed at preventing ICT-facilitated gender-based violence. Additionally, invest in raising awareness for the intersection between human rights and digital security, demonstrating how human rights must be taken seriously in both the offline and online spaces. This can come in many forms, including working closely with local communities and human rights organisations (e.g. feminist groups, LGBTIQ+ groups) to facilitate dialogue and sensitivity training regarding the needs of people marginalised based on gender and/or other factors;

3. CCDH, *PUBLIC SUPPORT FOR SOCIAL MEDIA REFORM: Assessing CCDH’s STAR Framework for social media regulation*, (16 August 2023), available at: <https://counterhate.com/research/public-support-for-social-media-reform-star/>.

- 12 Implement and communicate stringent user codes of conduct across their platforms, ensuring their enforcement. Additionally, establish uniform content moderation standards that can effectively identify and address nuanced forms of online violence, while remaining sensitive to diverse cultural and linguistic contexts;
- 13 Improve the systems for reporting abuse so that victims of OGBV and racial discrimination can easily report it and track the progress of the reports;
- 14 Publish regular information on official websites regarding the legal basis of requests made by governments and other third parties and regarding the content or accounts restricted or removed under the company's own policies and community guidelines, and establish clear, comprehensive grievance mechanisms that allow governing bodies and civil society members to dispute restrictions or removals of content and accounts. Aside from being clear and comprehensive, these mechanisms must have efficient, effective, and bias-trained systems of humans and/or electronic systems ready to receive and handle the grievances.;
- 15 When appropriate, consider less-invasive alternatives to content removal, such as demotion of content, labelling, fact-checking, promoting more authoritative sources, and implementing design changes that improve civic discussions;
- 16 Engage in continuous dialogue with civil society to understand the human rights impacts of current and potential sanctions, and avoid overcompliance in policy and practice;
- 17 Ensure that the results of human rights impact assessments and public consultations are made public;
- 18 Ensure that any requests, orders and commands to remove content must be based on validly enacted law, subject to external and independent oversight, and demonstrates a necessary as well as proportionate means to achieve one or more aims;
- 19 Organise task forces and initiate proactive initiatives to safeguard LGBTIQ+, women, girls and other concerned minorities against specific forms of abuse, (e.g. the non-consensual sharing of intimate images, including revenge porn), doxxing, hate speech, and overall gender-based violence;
- 20 Carry out routine assessments of human rights impacts and provide comprehensive transparency reports on measures taken to address the against marginalised communities (e.g. e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn);
- 21 Conduct assessments and due diligence processes to determine the impact of business activities on users, with respect to online freedom. Ensure meaningful and inclusive stakeholder engagement, with no one left behind.
- 22 Integrate subjects related to OGBV and healthy relationships, consent, bullying and online safety in school curricula, through a Department of Education campaign against OGBV.
- 23 Provide gender training for law enforcement officers for them to investigate OGBV cases and prosecute perpetrators.

Recommendations to Civil Society

- 1 Set up an independent multi-stakeholder body with the cooperation of various sectors to monitor and provide recommendations on trends in, and individual cases of digital rights abuses;
- 2 Work alongside governments and other stakeholders, to generate dialogue on issues and ensure accountability of government measures especially when it comes to issues related to democracy and human rights;
- 3 Support the independent evaluation and analysis of substantive aspects, including the use of the principles of necessity and proportionality through established global standards, and the impact of responses on society and economy;
- 4 Hold implementing authorities and officials liable for the misuse of their powers or information obtained, while carrying out their duties in the existing legal framework;
- 5 Strengthen understanding and solidarity among underprivileged people (e.g. class solidarity, solidarity among women and others marginalised based on gender, understanding among different ethnic groups within a jurisdiction);
- 6 Promote a safe and respectful environment for free online expression;
- 7 Continue to increase knowledge on digital security through training and capacity building programs, and actively carry out training on media literacy, including how to verify information to be true;
- 8 Continue to conduct awareness campaigns to educate individuals and communities about the various forms of gender-based violence, its impact on survivors, and the importance of promoting a safe and respectful online environment;
- 9 Advocate for the implementation and enforcement of robust laws and policies that criminalise all forms of gender-based violence, including OGBV;
- 10 Develop and implement digital literacy programs that equip individuals, especially women and marginalised communities, with skills to navigate online platforms safely, recognise and respond to online harassment, and protect their privacy;
- 11 Create and participate in grassroots, community-led initiatives to safeguard LGBTIQ+, women, girls and other concerned minorities against specific forms of abuse (e.g. the non-consensual sharing of intimate images, including revenge porn), doxxing, hate speech, and overall gender-based violence. Wherever possible, mobilise these initiatives to hold governments, MPs, and corporations accountable.
- 12 Have specialised support services and helplines for the survivors of OGBV, including counselling. Advocate for data collection and collect disaggregated data on OGBV when running prevention and response programmes.
- 13 Collaborate with social media platforms and technology companies to develop and enforce policies and mechanisms that effectively address OGBV.

Glossary

Abolition: putting an end to something by law

Appeal: the resort to a higher court to review the decision of a lower court, or to a court to review the order of an administrative agency

Arresto mayor: In Philippine criminal law, a sentence of imprisonment with a full range of one month and a day to six months

Attorney: a person legally appointed or empowered to act on behalf of another person

Bail: a sum of money paid by a defendant upon release to ensure later appearance in court

Bill: a statute in draft, before it becomes law

Charge: the specific statement of the crime accused to a party in the indictment or criminal complaint in a criminal case

Chilling effect: suppression of free speech and legitimate forms of dissent among a population due to fear of repercussion

Customary international law: international obligations arising from established international practices accepted as the norm

Conviction: an adjudication or formal declaration of a criminal defendant's guilt

Damages: a sum of money the law imposes to compensate a loss or injury

Defendant: someone who is being sued or accused of committing a crime

Distributed Denial-of-Service (DDoS) attack: a malicious attempt to disrupt normal traffic to a website or targeted server

De facto: Latin for "in fact." Phrase to show that that a state of affairs is true in fact, but not officially sanctioned

Directive: a set of instructions, guidelines, decisions or regulations issued by an official body outlining how a legal objective is to be achieved

Disenfranchisement: the removal of the rights and privileges inherent in an individual or group

Doxxing: publicly revealing identifying information about a person online

Entry into force: the coming into effect of a law or international agreement as to make it binding

Extradition: surrender by a country of a person charged with a crime in another country, usually under provisions of a treaty

Felony: a crime, characterised under federal law and state statutes as any offence punishable by imprisonment of over one year or death

Grievance mechanism: a formalised process, either judicial or non-judicial, by which a harm or cost suffered by a person can be compensated or remedied

Hoax: a trick or something else that is intended to deceive someone

Incommunicado detention: a situation of detention where a person is denied access to family members, an attorney or independent physician

Indictment: a formal written accusation stating that a person is being charged with a crime and must undergo a criminal trial

Injunction: a court order by which a person is ordered to perform, or restrain from performing, a certain act

Lawsuit: a disagreement between people or organisations that is brought to a court of law for a decision

Libel: a published false statement that is damaging to a person's reputation

Moratorium: a delay or suspension of an activity or law until further consideration

Perjury: the intentional act of swearing a false oath or falsifying an affirmation to tell the truth, whether spoken or in writing, concerning matters material to an official proceeding

Persecution: severe discrimination that results in the denial or infringement of fundamental rights

Phishing: a technique to trick a person into disclosing sensitive data through the use of deceptive emails or websites

Pre-trial detention: the detaining of an accused person in a criminal case before the trial has taken place

Prisión correccional: In Philippine criminal law, a sentence of imprisonment with a full range of six months and one day to six years

Prisión mayor: In Philippine criminal law, a sentence of major imprisonment with a full range of from six years and one day to twelve years

Probation: an alternative to imprisonment allowing a convicted person to stay in the community, usually under conditions and supervision of a probation officer

Prosecution: the initiation of criminal proceedings against a person accused of a crime

Ratification: an international act whereby a state expresses its consent to be bound to a treaty by an exchange or deposit of requisite instruments

Redress: relief or remedy or a means of seeking relief or remedy

Red-tagging: a harmful practice that targets people who often end up being harassed or even killed

Reverse onus: a legal provision that shifts the burden of proof onto a specified individual, normally the defendant, to disprove an element of an information

Self-censorship: withholding of one's true opinion from others in the absence of formal obstacles

Slander: false oral statements which damages the reputation of others

SLAPP suit: a civil claim filed against an individual or organisation to dissuade criticism, or intimidate or harass into silence

Smear campaign: a planned attempt to harm the reputation of a person or company by telling lies about them

Status quo: state of affairs as it exists at a particular time, normally one that precedes a controversy

Statute of limitations: a law that sets the maximum time that parties have to initiate legal proceedings from the date of an alleged offence

Sub judice contempt: a form of law that protects a person's right to a fair hearing by preventing the publication of material or comment which may improperly influence a jury or witness

Summons: a document issued by a court notifying someone that they are being sued or required to appear in court

Uphold (of a decision): to agree with a decision made earlier by a lower court

Writ: a written order issued by an administrative or judicial body

Endnotes

1. Freedom House, Freedom In The World 2020: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-world/2020>; Freedom House, Freedom On The Net 2020: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2020>; Reporters sans frontières, RSF's World Press Freedom Index, 2020, (n.d.), available at: <https://rsf.org/en/index?year=2020>; Freedom House, FREEDOM IN THE WORLD 2021: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-world/2021>; Freedom House, FREEDOM On The Net 2021: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2021>; Reporters sans frontières, RSF's World Press Freedom Index, 2021, (n.d.), available at: <https://rsf.org/en/index?year=2021>; Freedom House, FREEDOM IN THE WORLD 2022: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-world/2022>; Freedom House, FREEDOM On The Net 2022: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2022>; Reporters sans frontières, RSF's World Press Freedom Index, 2022, (n.d.), available at: <https://rsf.org/en/index?year=2022>; Freedom House, FREEDOM IN THE WORLD 2023: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-world/2023>; Freedom House, FREEDOM On The Net 2023: Indonesia, (n.d.), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2023>; Reporters sans frontières, RSF's World Press Freedom Index, 2023, (n.d.), available at: <https://rsf.org/en/index?year=2023>
2. Indonesia's Constitution of 1945, Reinstated in 1959, with Amendments through 2002, available at: https://www.constituteproject.org/constitution/Indonesia_2002.pdf?lang=en
3. Law of the Republic of Indonesia Number 39 of 1999 on Human Rights, available at: https://www.peraturan.go.id/files2/uu-no-39-tahun-1999_terjemah.pdf
4. Office of the United Nations High Commissioner for Human Rights, Ratification Status for Indonesia, available at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=80&Lang=EN
5. ASEAN Parliamentarians for Human Rights, Indonesia should set example on safeguarding digital rights ahead of elections, Southeast Asian MPs say, (30 May 2023), available at: <https://aseanmp.org/2023/05/30/indonesia-should-set-example-on-safeguarding-digital-rights-ahead-of-elections-southeast-asian-mps-say/>
6. Media Defence, Explaining the Issues: Sedition, (13 November 2013), available at: <https://www.media-defence.org/news/explaining-the-issues-sedition/>
7. Jurnal Kawistara, RELIGIOUS BLASPHEMY AND MONITORY SOCIETY IN INDONESIAN DIGITAL AGE, (2019), available at: <https://journal.ugm.ac.id/kawistara/article/view/41169>
8. Law of The Republic of Indonesia Number 1 Of 2023 on Criminal Code, available at: <https://the-world-is-watching.org/wp-content/uploads/2023/02/2023-Indonesia-Penal-Code.pdf>; Law Number 1 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, available at: <https://peraturan.go.id/law>; Manushya Foundation, Joint Solidarity Statement: Unmasking Digital Oppression: Second Revisions to Indonesia's EIT Law Fuelling Online Repression, (30 November 2023), available at: <https://www.manushyafoundation.org/unmaskingdigitaloppression>; Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>;
9. Butt, S. (2023). Indonesia's new Criminal Code: indigenising and democratising Indonesian criminal law? *Griffith Law Review*, 32(2), 190–214. <https://doi.org/10.1080/10383441.2023.2243772>
10. Law of The Republic of Indonesia Number 1 Of 2023 on Criminal Code, available at: <https://the-world-is-watching.org/wp-content/uploads/2023/02/2023-Indonesia-Penal-Code.pdf>; Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>; Hukum Online, New Indonesian Criminal Law Code to Come into Force by 2 January 2026, (4 January 2023), available at: <https://pro.hukumonline.com/a/lt63b-52cdab1027/new-indonesian-criminal-law-code-to-come-into-force-by-2-january-2026/>
11. Indonesian Institute the Independent Judiciary (Lembaga Kajian dan Advokasi Independensi Peradilan (LeIP)), Protecting Expression Criminal and Human Rights Law Analysis of Court Judgements in Indonesia, (2023), available at: <https://leip.or.id/wp-content/uploads/2023/06/eBook-Protection-Expression-Criminal-and-Human-Rights-Law-Analysis-of-Court-Judgements-in-Indonesia.pdf>; Carter-Ruck, Defamation and Privacy Law in Indonesia, (n.d.), available

- at: [https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-indonesia/#:~:text=Under%20Article%20310%20of%20the,certain%20matter%3B%20and%20\(iv\)](https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-indonesia/#:~:text=Under%20Article%20310%20of%20the,certain%20matter%3B%20and%20(iv))
12. Indonesian Institute the Independent Judiciary (Lembaga Kajian dan Advokasi Independensi Peradilan (LeIP)), Protecting Expression Criminal and Human Rights Law Analysis of Court Judgements in Indonesia, (2023), available at: <https://leip.or.id/wp-content/uploads/2023/06/eBook-Protection-Expression-Criminal-and-Human-Rights-Law-Analysis-of-Court-Judgements-in-Indonesia.pdf>; Carter-Ruck, Defamation and Privacy Law in Indonesia, (n.d)., available at: [https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-indonesia/#:~:text=Under%20Article%20310%20of%20the,certain%20matter%3B%20and%20\(iv\)](https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-indonesia/#:~:text=Under%20Article%20310%20of%20the,certain%20matter%3B%20and%20(iv))
 13. Indonesian Institute the Independent Judiciary (Lembaga Kajian dan Advokasi Independensi Peradilan (LeIP)), Protecting Expression Criminal and Human Rights Law Analysis of Court Judgements in Indonesia, (2023), available at: <https://leip.or.id/wp-content/uploads/2023/06/eBook-Protection-Expression-Criminal-and-Human-Rights-Law-Analysis-of-Court-Judgements-in-Indonesia.pdf>
 14. Amnesty International Indonesia, Indonesia: Landmark court decision nullifies defamation articles, (22 March 2024), available at: <https://www.amnesty.id/kabar-terbaru/siaran-pers/indonesia-landmark-court-decision-nullifies-defamation-articles/03/2024/>
 15. Law of The Republic of Indonesia Number 1 Of 2023 on Criminal Code, available at: <https://the-world-is-watching.org/wp-content/uploads/2023/02/2023-Indonesia-Penal-Code.pdf>; Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>; EngageMedia, Revisiting Problematic Articles in the Indonesian Criminal Code Before Its Enactment, (15 December 2023), available at: <https://engagemedia.org/2023/indonesia-criminal-code/>; Lembaga Bantuan Hukum Masyarakat, Pembatasan oleh Negara yang Melampaui Batas: Legal Opinion tentang Hak Kebebasan Berpendapat dalam KUHP, (26 January 2024), available at: <https://lbhmasyarakat.org/4124/>
 16. Law of The Republic of Indonesia Number 1 Of 2023 on Criminal Code, available at: <https://the-world-is-watching.org/wp-content/uploads/2023/02/2023-Indonesia-Penal-Code.pdf>; Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>; EngageMedia, Revisiting Problematic Articles in the Indonesian Criminal Code Before Its Enactment, (15 December 2023), available at: <https://engagemedia.org/2023/indonesia-criminal-code/>; Lembaga Bantuan Hukum Masyarakat, Pembatasan oleh Negara yang Melampaui Batas: Legal Opinion tentang Hak Kebebasan Berpendapat dalam KUHP, (26 January 2024), available at: <https://lbhmasyarakat.org/4124/>
 17. International Commission of Jurists, Indonesia: Criminalization of disinformation threatens freedom of expression, (12 January 2023), available at: <https://www.icj.org/indonesia-criminalization-of-disinformation-threatens-freedom-of-expression/>
 18. Aliansi Jurnalis Independen, Articles on fake news and defamation in the Criminal Code have been declared unconstitutional by the Indonesian Constitutional Court, (17 April 2024), available at: <https://aji.or.id/informasi/articles-fake-news-and-defamation-criminal-code-have-been-declared-unconstitutional>
 19. Law of The Republic of Indonesia Number 1 Of 2023 on Criminal Code, available at: <https://the-world-is-watching.org/wp-content/uploads/2023/02/2023-Indonesia-Penal-Code.pdf>; Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>; EngageMedia, Revisiting Problematic Articles in the Indonesian Criminal Code Before Its Enactment, (15 December 2023), available at: <https://engagemedia.org/2023/indonesia-criminal-code/>; Lembaga Bantuan Hukum Masyarakat, Pembatasan oleh Negara yang Melampaui Batas: Legal Opinion tentang Hak Kebebasan Berpendapat dalam KUHP, (26 January 2024), available at: <https://lbhmasyarakat.org/4124/>
 20. The University of Melbourne, Half-hearted progress: religious freedom after the new Criminal Code, (17 January 2023), available at: <https://indonesiaatmelbourne.unimelb.edu.au/half-hearted-progress-religious-freedom-after-the-new-criminal-code/#:~:text=The%20most%20well%2Dknown%20is,criminal%20code%2C%20under%20Article%20156a.>

21. Human Rights Watch, Indonesia: New Criminal Code Disastrous for Rights, (8 December 2022), available at: <https://www.hrw.org/news/2022/12/08/indonesia-new-criminal-code-disastrous-rights>
22. Edelman Global Advisory, Indonesia's Parliament Passes New Criminal Code Law (KUHP), (8 December 2022), available at: <https://www.edelman-globaladvisory.com/insights/Indonesias-Parliament-Passes-New-Criminal-Code-Law>
23. Office of the High Commissioner for Human Rights, Indonesia: Stop judicial harassment of human rights defenders – UN expert, (26 November 2021), available at: <https://www.ohchr.org/en/press-releases/2021/11/indonesia-stop-judicial-harassment-human-rights-defenders-un-expert>
24. Manushya Foundation, Indonesia's New Criminal Code Is a Massive Threat to Human Rights, (9 December 2022), available at: <https://www.manushyafoundation.org/post/indonesia-s-new-criminal-code-is-a-massive-threat-to-human-rights>; Manushya Foundation, Joint Solidarity Statement: Indonesia: Stop Abusing Cyberlaw and Criminal Defamation to Harass Human Rights Defenders Fatia Maulidiyanti and Haris Azhar & to Stop Them from Speaking Truth to Power!, (21 September 2021), available at: <https://www.manushyafoundation.org/joint-solidarity-statement-indonesia-stop-abusing-cyber-law-and-criminal-defamation>; Manushya Foundation, Human Rights Defenders' freedom of expression must be respected offline and online!, (9 February 2022), available at: <https://www.manushyafoundation.org/post/human-rights-defenders-freedom-of-expression-must-be-respected-offline-and-online>
25. SAFENet, Revisi Kedua UU ITE: Masih Mempertahankan Pasal-Pasal Karet yang lama, Menambah Pasal Baru yang Sangat berbahaya, (4 January 2023), available at: <https://safenet.or.id/id/2024/01/revisi-kedua-uu-ite-masih-mempertahankan-pasal-pasal-karet-yang-lama-menambah-pasal-baru-yang-sangat-berbahaya/>
26. Carter Rack, Defamation and Privacy Law in Indonesia, (n.d), available at: <https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-indonesia/>
27. Makarim & Taira S Counsellors at Law, Second Amendment to Indonesia's ITE Law: What's Changed?, (February 2024), available at: <https://www.makarim.com/news/second-amendment-to-indonesia-s-ite-law-what-s-changed>
28. Makarim & Taira S Counsellors at Law, Second Amendment to Indonesia's ITE Law: What's Changed?, (February 2024), available at: <https://www.makarim.com/news/second-amendment-to-indonesia-s-ite-law-what-s-changed>
29. Law Number 1 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, available at: <https://peraturan.go.id/law>; Amnesty Indonesia, Pernyataan sikap Koalisi Serius ITE terkait tuntutan pencemaran nama baik terhadap aktivis pembela HAM Fatia Maulidiyanti dan Haris Azhar, (16 November 2023), available at: <https://www.amnesty.id/pernyataan-sikap-koalisi-serius-ite-terkait-tuntutan-pencemaran-nama-baik-terhadap-aktivis-pembela-ham-fatia-maulidiyanti-dan-haris-azhar/>; Manushya Foundation, Joint Solidarity Statement: Unmasking Digital Oppression: Second Revisions to Indonesia's EIT Law Fuelling Online Repression, (30 November 2023), available at: <https://www.manushyafoundation.org/unmaskingdigitaloppression>
30. Law Number 1 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, available at: <https://peraturan.go.id/law>
31. Law Number 1 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, available at: <https://peraturan.go.id/law>
32. Law Number 1 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, available at: <https://peraturan.go.id/law>; Manushya Foundation, JOINT SOLIDARITY STATEMENT Unmasking Digital Oppression: Second Revisions to Indonesia's EIT Law Fuelling Online Repression, (30 November 2023), available at: <https://www.manushyafoundation.org/unmaskingdigitaloppression>
33. SAFENet, Kasus Ibu Nuril, (30 July 2019), available at: <https://safenet.or.id/id/2017/07/kasus-ibu-nuril/>; Manushya Foundation, JOINT SOLIDARITY STATEMENT Unmasking Digital Oppression: Second Revisions to Indonesia's EIT Law Fuelling Online Repression, (30 November 2023), available at: <https://www.manushyafoundation.org/unmaskingdigitaloppression>
34. BBC, Kasus Baiq Nuril: Perempuan yang dipidanakan karena merekam percakapan mesum akan 'tagih amnesti' ke Jokowi, (15 July 2019), available at: <https://www.bbc.com/indonesia/indonesia-48878086>
35. United Nations Convention on the Elimination of All Forms of Discrimination against Women, available at: <https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/cedaw.pdf>

36. SAFEnet, Revisi Kedua UU ITE: Masih Mempertahankan Pasal-Pasal Karet yang lama, Menambah Pasal Baru yang Sangat berbahaya, (4 January 2023), available at: <https://safenet.or.id/id/2024/01/revisi-kedua-uu-ite-masih-mempertahankan-pasal-pasal-karet-yang-lama-menambah-pasal-baru-yang-sangat-berbahaya/>
37. Tempo, Kelompok Sipil Sorot Pasal-pasal Berbahaya dalam Revisi UU ITE Jilid 2, (5 January 2024), available at: <https://nasional.tempo.co/read/1817435/kelompok-sipil-sorot-pasal-pasal-berbahaya-dalam-revisi-uu-ite-jilid-2>
38. Manushya Foundation, JOINT SOLIDARITY STATEMENT : Unmasking Digital Oppression: Second Revisions to Indonesia's EIT Law Fuelling Online Repression, (30 November 2023), available at: <https://www.manushyafoundation.org/unmasking-digitaloppression>; Manushya Foundation, Joint Solidarity Statement: Indonesia: Stop Abusing Cyberlaw and Criminal Defamation to Harass Human Rights Defenders Fatia Maulidiyanti and Haris Azhar & to Stop Them from Speaking Truth to Power!, (21 September 2021), available at: <https://www.manushyafoundation.org/joint-solidarity-statement-indonesia-stop-abusing-cyber-law-and-criminal-defamation>
39. Minister of Communication and Information of the Republic of Indonesia - Regulation Number 10 of 2021 (MR10) on Amendments to Regulation of the Minister of Communication and Information of the Republic of Indonesia - Regulation Number 5 Year 2020 (MR5), available at: https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020; Manushya Foundation, Joint Statement: Global Coalition of NGOs: Repeal MR5 and its amendment MR10 in Indonesia, (4 July 2022), available at: <https://www.manushyafoundation.org/joint-statement-repeal-mr5-and-its-amendment-mr10-in-indonesia>; Manushya Foundation, Joint Statement: Call on Indonesian Ministry of Communication and Information Technology to Suspend the Implementation of Permenkominfo No. 5/2020 (MR5/2020), (28 May 2021), available at: <https://www.manushyafoundation.org/joint-statement-call-on-indonesian-ministry>
40. Minister of Communication and Information of the Republic of Indonesia - Regulation Number 10 of 2021 (MR10) on Amendments to Regulation of the Minister of Communication and Information of the Republic of Indonesia - Regulation Number 5 Year 2020 (MR5), available at: https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020; Manushya Foundation, Joint Statement: Global Coalition of NGOs: Repeal MR5 and its amendment MR10 in Indonesia, (4 July 2022), available at: <https://www.manushyafoundation.org/joint-statement-repeal-mr5-and-its-amendment-mr10-in-indonesia>; Manushya Foundation, Joint Statement: Call on Indonesian Ministry of Communication and Information Technology to Suspend the Implementation of Permenkominfo No. 5/2020 (MR5/2020), (28 May 2021), available at: <https://www.manushyafoundation.org/joint-statement-call-on-indonesian-ministry>
41. Minister of Communication and Information of the Republic of Indonesia - Regulation Number 5 Year 2020 (MR5), available at: https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020; ARTICLE 19, Indonesia: Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5), (September 2021), available at: <https://www.article19.org/wp-content/uploads/2021/09/Legal-Analysis-Indonesia-Ministerial-Regulation-5.pdf>
42. Manushya Foundation, Joint Statement: Call on Indonesian Ministry of Communication and Information Technology to Suspend the Implementation of Permenkominfo No. 5/2020 (MR5/2020), (28 May 2021), available at: <https://www.manushyafoundation.org/joint-statement-call-on-indonesian-ministry>; Manushya Foundation, Joint Statement: Global Coalition of NGOs: Repeal MR5 and its amendment MR10 in Indonesia, (4 July 2022), available at: <https://www.manushyafoundation.org/joint-statement-repeal-mr5-and-its-amendment-mr10-in-indonesia>
43. ARTICLE 19, Indonesia: Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5), (September 2021), available at: <https://www.article19.org/wp-content/uploads/2021/09/Legal-Analysis-Indonesia-Ministerial-Regulation-5.pdf>
44. Manushya Foundation, Joint Statement: Call on Indonesian Ministry of Communication and Information Technology to Suspend the Implementation of Permenkominfo No. 5/2020 (MR5/2020), (28 May 2021), available at: <https://www.manushyafoundation.org/joint-statement-call-on-indonesian-ministry>
45. Aliansi Jurnalis Independen, Indonesia: Ministerial Regulation 5 Threatens to Restrict Press and Internet Freedom, (25 July 2022), available at: <https://aji.or.id/read/press-release/1410/indonesia-ministerial-regulation-5-threatens-to-restrict-press-and-internet-freedom.html>
46. Manushya Foundation, Joint Statement: Global Coalition of NGOs: Repeal MR5 and its amendment

- MR10 in Indonesia, (4 July 2022), available at: <https://www.manushyafoundation.org/joint-statement-repeal-mr5-and-its-amendment-mr10-in-indonesia>: Manushya Foundation, Joint Statement: Call on Indonesian Ministry of Communication and Information Technology to Suspend the Implementation of Permenkominfo No. 5/2020 (MR5/2020), (28 May 2021), available at: <https://www.manushyafoundation.org/joint-statement-call-on-indonesian-ministry>
47. Freedom House, Freedom on the Net 2021: Indonesia, (2021), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2021>; Freedom House, Freedom on the Net 2022: Indonesia, (2022), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2022>; Freedom House, Freedom on the Net 2023: Indonesia, (2023), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2023>
 48. Reporters Without Borders, Indonesia, (n.d.), available at: <https://rsf.org/en/indonesia>
 49. Patroli Siber, Number of Police Reports Made by the Public, (n.d.), available at: <https://patrolisiber.id/statistic>
 50. Detik, Maret 2021 Ada Ribuan Laporan Kejahatan Siber, Didominasi Laporan Konten SARA, (18 April 2021), available at: <https://inet.detik.com/law-and-policy/d-5536679/maret-2021-ada-ribuan-laporan-kejahatan-siber-didominasi-laporan-konten-sara>
 51. Patroli Siber, Number of Police Reports Made by the Public, (n.d.), available at: <https://patrolisiber.id/statistic>
 52. Patroli Siber, Number of Police Reports Made by the Public, (n.d.), available at: <https://patrolisiber.id/statistic>
 53. Tempo, Ada Ribuan Laporan UU ITE, SAFEnet: Polisi Sibuk Urusi Pencemaran Nama Baik, (5 March 2021), available at: <https://nasional.tempo.co/read/1438925/ada-ribuan-laporan-uu-ite-safenet-polisi-sibuk-urusi-pencemaran-nama-baik>
 54. SAFEnet, Digital Rights in Indonesia Situation Report 2021: The Pandemic Might be Under Control, but Digital Repression Continues, (February 2022), available at: <https://safenet.or.id/in-indonesia-digital-repression-is-keep-continues/>
 55. Amnesty International, Indonesia: Human Rights Defenders accused of Defamation, (1 November 2021), available at: <https://www.amnesty.org.uk/urgent-actions/human-rights-defenders-accused-defamation>
 56. Amnesty Indonesia, Pernyataan sikap Koalisi Serius ITE terkait tuntutan pencemaran nama baik terhadap aktivis pembela HAM Fatia Maulidiyanti dan Haris Azhar, (16 November 2023), available at: <https://www.amnesty.id/pernyataan-sikap-koalisi-serius-ite-terkait-tuntutan-pencemaran-nama-baik-terhadap-aktivis-pembela-ham-fatia-maulidiyanti-dan-haris-azhar/>
 57. Yayasan Lembaga Bantuan Hukum Indonesia (YLBHI), KOALISI SERIUS Mendesak Penundaan Pengesahan Revisi Kedua UU ITE, (23 November 2023), available at: <https://ylbhi.or.id/informasi/siaran-pers/koalisi-serius-mendesak-penundaan-pengesahan-revisi-kedua-uu-ite/>
 58. SAFEnet, Revisi UU ITE Total Sebagai Solusi, (10 March 2021), available at: <https://id.safenet.or.id/2021/03/revisi-uu-ite-total-sebagai-solusi/>
 59. Forum-Asia and KontraS, Joint Analysis on the situation of defenders in Asia, (21 March 2023), available at: <https://forum-asia.org/?p=37933>
 60. SAFEnet, Kasus Mohamad Sadli, (1 February 2020), available at: <https://id.safenet.or.id/2020/02/kasus-mohamad-sadli/>
 61. Amnesty International, Indonesia: Lecturer Sentenced for WhatsApp Message: Saiful Mahdi, (14 July 2021), available at: <https://www.amnesty.org/en/documents/asa21/4461/2021/en/>; CIVICUS Monitor, Human Rights Defenders, Critics Targeted In Indonesia While Protests On Papua Repressed, (21 September 2021), available at: <https://monitor.civicus.org/updates/2021/09/21/human-rights-defenders-critics-targeted-indonesia-while-protests-papua-repressed/>
 62. Tribun News, Siapa Saiful Mahdi? Dosen Unsyiah Kuala yang Diberi Amnesti oleh Jokowi atas Kasus UU ITE, (5 October 2021), available at: <https://www.tribunnews.com/regional/2021/10/05/siapa-saiful-mahdi-dosen-unsyiah-kuala-aceh-yang-diberi-amnesti-oleh-jokowi-atas-kasus-uu-ite>
 63. The Online Citizen, How urgent is the revision of Indonesia's Electronic Information and Transaction Law?, (26 February 2021), available at: <https://www.theonlinecitizen.com/2021/02/26/how-urgent-is-the-revision-of-indonesias-electronic-information-and-transaction-law/>; Voice of Indonesia, Marco Kusumawijaya, Ex TGUPP Anies, Is Investigated By The Police About Suspected Threats Through Social Media, (2 February 2021), available at: <https://voi.id/en/bernas/30324/marco-kusumawijaya-ex-tgupp-anies-is-investigated-by-the-police-about-suspected-threats-through-social-media>

64. Suara News, Marco Kusumawijaya: Pemerintah Coba Mengakses Akun Saya, Apa Benar?, (8 October 2021), available at: <https://www.suara.com/news/2021/10/08/095731/marco-kusumawijaya-pemerintah-coba-mengakses-akun-saya-apa-benar>
65. SAFEnet, Digital Rights Situation Report Indonesia 2020: Digital Repression Amid the Pandemic, (5 May 2021), available at: <https://safenet.or.id/digital-situation-report-2020/>
66. Human Rights Asia, INDONESIA: Labor Activist, after delivering a public speech, is criminally charged under Articles of Criminal Defamation, (22 January 2021), available at: <http://www.humanrights.asia/news/ahrc-news/AHRC-UAC-001-2021/>; Freedom House, Freedom on the Net: Indonesia, (2021), available at: <https://freedomhouse.org/country/indonesia/freedom-net/2021>
67. JATAM, Economic-Political Military Placement in Papua: The Case of Intan Jaya, (18 August 2021), available at : <https://www.jatam.org/en/political-economy-of-military-deployment-in-papua/>; Manushya Foundation, Joint Solidarity Statement, Indonesia: Stop Abusing Cyberlaw and Criminal Defamation to Harass Human Rights Defenders Fatia Maulidiyanti and Haris Azhar & to Stop Them from Speaking Truth to Power!, (21 September 2021), available at: <https://www.manushyafoundation.org/joint-solidarity-statement-indonesia-stop-abusing-cyber-law-and-criminal-defamation>
68. Amnesty International, Indonesia: Human rights defenders accused of defamation: Haris Azhar and Fatia Maulidiyanti, (1 November 2021), available at: <https://www.amnesty.org/en/documents/asa21/4932/2021/en/>
69. Antara News, Haris Azhar-Fatia Maulidiyanti diperiksa selama enam jam, (18 January 2022), available at: <https://www.antaraneews.com/berita/2650997/haris-azhar-fatia-maulidiyanti-diperiksa-selama-enam-jam>
70. KontraS, Haris and Fatia Victims of Criminalization of Public Officials for Business Scandals in Papua, (19 March 2022), available at: <https://kontras.org/en/2022/03/19/haris-and-fatia-victims-of-criminalization-of-public-officials-for-business-scandals-in-papua/>; CNN Indonesia, Haris Azhar & Fatia Kembali Diperiksa Sebagai Tersangka di Kasus Luhut, (1 November 2022), available at: <https://www.cnnindonesia.com/nasional/20221101090352-12-867866/haris-azhar-fatia-kembali-diperiksa-sebagai-tersangka-di-kasus-luhut>; Benar News, Indonesian activists stand trial in defamation case filled by cabinet minister, (3 April 2023), available at: <https://www.benarnews.org/english/news/indonesian/defamation-case-04032023155139.html>
71. Manushya Foundation, Joint Statement: Solidarity for Human Rights Defenders Fatia Maulidiyanti and Haris Azhar, (22 November 2023), available at: <https://www.manushyafoundation.org/fatiharisglobal-solidarity>
72. Tempo, Haris Azhar, Fatia Maulidiyanti Acquitted in Defamation Trial; Luhut Comments, (8 January 2024), available at: <https://en.tempo.co/read/1818660/haris-azhar-fatia-maulidiyanti-acquitted-in-defamation-trial-luhut-comments>
73. Kompas, Haris Azhar-Fatia Tersangka Dinilai Bukti Pejabat Sulit Terima Kritik, (21 March 2022), available at: <https://nasional.kompas.com/read/2022/03/21/15073751/haris-azhar-fatia-ter-sangka-dinilai-bukti-pejabat-sulit-terima-kritik>
74. Amnesty International, Indonesia 2022, (n.d.), available at: <https://www.amnesty.org/en/location/asia-and-the-pacific/south-east-asia-and-the-pacific/indonesia/report-indonesia/#endnote-6>
75. Amnesty International, Stop criminalizing the right to freedom of expression, (14 April 2022), available at: <https://www.amnesty.id/stop-criminalizing-the-right-to-freedom-of-expression/>
76. Jakarta Globe, Former Democratic Party Politician Gets Five Months in Prison for Allah Tweet, (19 April 2022), available at: <https://jakartaglobe.id/news/former-democratic-party-politician-gets-five-months-in-prison-for-allah-tweet>
77. iFex, Indonesia: AJI chairperson targeted in hacking and disinformation attack, (25 February 2022), available at: <https://ifex.org/indonesia-aji-chairperson-targeted-in-hacking-and-disinformation-attacks/>
78. SAFEnet, Digital Rights Situation Report Indonesia 2020: Digital Repression Amid the Pandemic, (2021), available at: <https://safenet.or.id/digital-situation-report-2020/>
79. SAFEnet, Digital Rights in Indonesia Situation Report 2021: The Pandemic Might be Under Control, but Digital Repression Continues, (n.d.), available at: <https://safenet.or.id/in-indonesia-digital-repression-is-keep-continues/>
80. SAFEnet, Digital Rights in Indonesia Situation Report 2022: The Collapse of Our Digital Rights, (March 2023), available at: <https://safenet.or.id/2023/03/the-digital-rights-situation-in-indonesia-had-worsened/>
81. SAFEnet, Journalist Safety Committee Condemns the Criminalization of Journalists with the ITE Law, (18 February 2020), available at: <https://id.safenet.or.id/2020/02/rilis-pers-komite-keselamatan-jurnalis-kecam-pemidanaan-jurnalis-dengan-uu-ite/>

82. Archyworldys, Three Journalists Have Been Imprisoned in the Jokowi-Ma'ruf Era Using the Snare of the ITE Law, (26 November 2021), available at: <https://www.archyworldys.com/three-journalists-have-been-imprisoned-in-the-jokowi-maruf-era-using-the-snare-of-the-ite-law/>; CNN Indonesia, *Jurnalis Divonis 3 Bulan Penjara Usai Bongkar Dugaan Korupsi di Palopo*, (23 November 2021), available at: <https://www.cnnindonesia.com/nasional/20211123161901-12-725045/jurnalis-divonis-3-bulan-penjara-usai-bongkar-dugaan-korupsi-di-palopo>
83. Suara News, *Di Hari Kemerdekaan, Jurnalis Diananta Putra Sumedi Resmi Bebas*, (17 August 2020), available at: <https://www.suara.com/news/2020/08/17/200540/di-hari-kemerdekaan-jurnalis-diananta-putra-sumedi-resmi-bebas?page=all>
84. Manushya Foundation, *Indonesia: Small Business Owner Wahyu Dwi Nugroho's Conviction Challenges Free Speech*, (1 August 2023), available at: <https://www.manushyafoundation.org/post/indonesia-small-business-owner-wahyu-dwi-nugroho-s-conviction-challenges-free-speech>
85. The Jakarta Post, *New 'virtual police' adds to fears over loss of online civic space, civil freedoms*, (19 March 2021), available at: <https://www.thejakartapost.com/news/2021/03/19/new-virtual-police-adds-to-fears-over-loss-of-online-civic-space-civil-freedoms.html>; Tempo, *Virtual Police Issue Warning to 200 Social Media Accounts*, (13 April 2021), available at: <https://en.tempo.co/read/1451994/virtual-police-issue-warning-to-200-social-media-accounts>
86. Association for Progressive Communication, *A COVID-19 power grab: Looming digital authoritarianism in Indonesia*, (26 October 2022), available at: <https://www.apc.org/en/news/covid-19-power-grab-looming-digital-authoritarianism-indonesia>
87. Reuters, *EXCLUSIVE Indonesia preparing tough new curbs for online platforms-sources'*, (23 March 2023), available at: <https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-sources-2022-03-23/>
88. Kontan, *Facebook, WhatsApp, Instagram, Netflix Sudah Daftar PSE, Google, YouTube Belum*, (20 July 2022), available at: <https://nasional.kontan.co.id/news/facebook-whatsapp-instagram-netflix-sudah-daftar-pse-google-youtube-belum>; *Bisnis.com*, *Google dan YouTube Sudah Daftar, Ini Dia PSE yang Belum Daftar ke Kominfo*, (24 July 2022), available at: <https://teknologi.bisnis.com/read/20220724/84/1558468/google-dan-youtube-sudah-daftar-ini-dia-pse-yang-belum-daftar-ke-kominfo>
89. Reuters, *Indonesia blocks Yahoo, Paypal, gaming websites over license breaches*, (2 August 2022), available at: <https://www.reuters.com/technology/indonesia-blocks-yahoo-paypal-gaming-websites-over-licence-breaches-2022-07-30/>
90. CNBC Indonesia, *Kominfo Ancam Blokir PSE yang Sudah Daftar, jika...*, (3 August 2022), available at: <https://www.cnbcindonesia.com/tech/20220803175637-37-360891/kominfo-ancam-blokir-pse-yang-sudah-daftar-jika>
91. Suara News, *Klaim untuk Lindungi Masyarakat, Menkominfo Sebut Pendaftaran PSE Tidak Terkait Data Pribadi*, (1 August 2022), available at: <https://www.suara.com/news/2022/08/01/121615/klaim-untuk-lindungi-masyarakat-menkominfo-sebut-pendaftaran-pse-tidak-terkait-data-pribadi>
92. Citizen Lab, *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, (16 December 2021), available at: <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>
93. Citizen Lab, *Running in Circles Uncovering the Clients of Cyberespionage Firm Circles*, (1 December 2020), available at: <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>
94. Benar News, *Whistle-blower: Indonesia may have used Israeli malware to spy on political opponents*, (12 June 2023), available at: <https://www.benarnews.org/english/news/indonesian/israeli-spyware-used-by-state-agencies-06122023115033.html>
95. Britannica, *Pegasus (spyware)*, (n.d.), available at: <https://www.britannica.com/topic/Pegasus-spyware>; Amnesty International, *Emergency update for all Apple users: Everything you need to know about Pegasus spyware*, (23 September 2021), available at: <https://www.amnesty.org.au/everything-you-need-to-know-about-pegasus-spyware/>
96. The Jakarta Post, *Israeli-made spyware Pegasus used in Indonesia since 2018, says IndonesiaLeaks*, (14 June 2023), available at: <https://www.thejakartapost.com/indonesia/2023/06/14/israeli-made-spyware-pegasus-used-in-indonesia-since-2018-says-indonesialeaks.htm>
97. Citizen Lab, *Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, (18 September 2018), available at: <https://citizenlab.ca/2018/09/hidden-and-seeking-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Human Rights Watch, *Human Rights Watch Among Pegasus Spyware Targets*, (26 January 2022), available at: <https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets>; Access

- Now, Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict, (25 May 2023), available at: <https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/>; Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks, (17 January 2022), available at: <https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>
98. Citizen Lab, Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, (18 September 2018), available at: <https://citizenlab.ca/2018/09/hidden-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Human Rights Watch, Human Rights Watch Among Pegasus Spyware Targets, (26 January 2022), available at: <https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets>; Access Now, Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict, (25 May 2023), available at: <https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/>; Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks, (17 January 2022), available at: <https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>
 99. New Naratif, Unlawful Surveillance in Southeast Asia, Pegasus Case, (7 December 2023), available at : <https://newnaratif.com/unlawful-surveillance-in-southeast-asia-pegasus-case/>
 100. New Naratif, Pegasus Spyware in Indonesia, (7 September 2023), available at : <https://newnaratif.com/pegasus-spyware-di-indonesia/>
 101. New Naratif, Unlawful Surveillance in Southeast Asia, Pegasus Case, (7 December 2023), available at : <https://newnaratif.com/unlawful-surveillance-in-southeast-asia-pegasus-case/>
 102. Manushya Foundation, Joint Solidarity Statement: Indonesia: Stop Using Pegasus to Scare People into Silence, (22 July 2023), available at: <https://www.manushyafoundation.org/indonesiastoppegasus>
 103. Indoleft, Rights group says cyber torture new threat against freedom of expression, (26 June 2020), available at: <https://www.indoleft.org/news/2020-06-26/rights-group-says-cyber-torture-new-threat-against-freedom-of-expression.html>; Protection International, 2020: A Dark Page in the History of Human Rights in Indonesia, (18 November 2021), available at: <https://www.protectioninternational.org/es/news/2020-dark-page-history-human-rights-indonesia>
 104. SAFEnet, Digital Rights Situation Report Indonesia 2020: Digital Repression Amid the Pandemic, (5 May 2021), available at: <https://safenet.or.id/digital-situation-report-2020/>
 105. SAFEnet, Digital Rights in Indonesia Situation Report 2021: The Pandemic Might be Under Control, but Digital Repression Continues, (February 2022), available at: <https://safenet.or.id/in-indonesia-digital-repression-is-keep-continues/>
 106. Indonesian Center for Environmental Law, [Siaran Pers Bersama] Peringatan Hari Pembela HAM Internasional 2021 Stop Kekerasan Terhadap Pembela HAM di Indonesia!, (9 December 2021), available at: <https://icel.or.id/berita/siaran-pers/siaran-pers-bersama-peringatan-hari-pembela-ham-internasional-2021-stop-kekerasan-terhadap-pembela-ham-di-indonesia/>
 107. SAFEnet, Digital Rights in Indonesia Situation Report 2022: The Collapse of Our Digital Rights, (March 2023), available at: <https://safenet.or.id/2023/03/the-digital-rights-situation-in-indonesia-had-worsened/>
 108. Reuters, Indonesian anti-graft activists complain of digital attacks, (25 May 2021), available at: <https://www.reuters.com/technology/indonesian-anti-graft-activists-complain-digital-attacks-2021-05-25/>
 109. Tempo, Hari Ini, Akun Medsos Pegawai KPK Tak Lolos TWK Kembali Kena Retas, (28 September 2021), available at: <https://nasional.tempo.co/read/1511279/hari-ini-akun-medsos-pegawai-kpk-tak-lolos-twk-kembali-kena-retas/full&view=ok>; Kompas, Pegawai KPK Tak Lolos TWK Dipecat, ICW Nilai Ada Keterlibatan Kelompok Tertentu, (27 May 2021), available at: <https://nasional.kompas.com/read/2021/05/27/05480791/pegawai-kpk-tak-lolos-twk-dipecat-icw-nilai-ada-keterlibatan-kelompok?page=all>
 110. SAFEnet, Digital Rights in Indonesia Situation Report 2021: The Pandemic Might be Under Control, but Digital Repression Continues, (February 2022), available at: <https://safenet.or.id/in-indonesia-digital-repression-is-keep-continues/>
 111. The Net Monitor, Indonesia, 2017, (2017), available at: <https://thenetmonitor.org/research/2017-global-internet-censorship/idn>
 112. A full list of blocked sites is available at: <https://trustpositif.kominfo.go.id/>
 113. Reuters, Indonesia blocks Yahoo, Paypal, gaming websites over licence breaches, (1 August 2022), available at: <https://www.reuters.com/technology/indonesia-blocks-yahoo-paypal-gaming-websites-over-licence-breaches-2022-07-30/#:~:text=Indonesia%20has%20blocked%20search%20en->

- gine%20website%20Yahoo%2C%20payments,on%20Saturday%2C%20sparkling%20a%20backlash%20on%20social%20media.
114. Khairil Zhafri (EngageMedia), Pradipa P Rasidi (EngageMedia), Siti Nurliza Samsudin (Sinar Project) and Kelly Koh (Sinar Project), iMAP Indonesia 2023 Internet Censorship Report, (2023), available at: <https://imap.sinarproject.org/reports/2023/imap-indonesia-2023-internet-censorship-report/imap-indonesia-2023-internet-censorship-report.pdf>
 115. Kompas, Berapa Gaji Buzzer di Indonesia, (12 December 2021), available at: <https://money.kompas.com/read/2021/12/12/204332926/berapa-gaji-buzzer-di-indonesia?page=all>
 116. Reuters, In Indonesia, Facebook and Twitter are 'buzzer' battlegrounds as elections loom, (13 March 2019), available at: <https://www.reuters.com/article/us-indonesia-election-socialmedia-insigh-idUSKBN1QU0AS>
 117. Reuters, Indonesian Army Wields Internet 'News' as a Weapon in Papua, (7 January 2020), available at: <https://www.reuters.com/article/us-indonesia-military-websites-insight/indonesian-army-wields-internet-news-as-a-weapon-in-papua-idUSKBN1Z7001>; Oxford Internet Institute, The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, (26 September 2019), available at: <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>
 118. RealkM Cooperative, How cyber troops are influencing what you think and know, (21 July 2017), available at: <https://realkm.com/2017/07/21/how-cyber-troops-are-influencing-what-you-think-and-know/>
 119. South China Morning Post, In Indonesia, fake UN accounts spewing anti-refugee hate feed rejection of Rohingya, (22 December 2023), available at: <https://www.scmp.com/week-asia/people/article/3246022/indonesia-fake-un-accounts-spewing-anti-refugee-hate-feed-rejection-rohingya>
 120. Facebook Transparency Report, Content restrictions, (n.d.), available at: <https://transparency.fb.com/data/content-restrictions/country/ID/>
 121. Google Transparency Report, Government requests to remove content, (n.d.), available at: <https://transparencyreport.google.com/government-removals/overview?hl=en>
 122. Twitter Transparency Report, Removal requests, (n.d.), available at: <https://transparency.twitter.com/en/reports/countries/id.html>
 123. TikTok Reports, Government Removal Requests Report, (n.d.), available at <https://www.tiktok.com/transparency/en/government-removal-requests-2022-1/>
 124. BBC Indonesia, Pemerintah Indonesia ajukan tiga syarat pencabutan blokir Telegram, (18 July 2017), available at: <https://www.bbc.com/indonesia/indonesia-40634402>; The University of Melbourne, Indonesia's Telegram ban: who's the real target?, (24 July 2017), available at: <https://indonesiaat-melbourne.unimelb.edu.au/indonesias-telegram-ban-whos-the-real-target/>
 125. Ministry of Communication and Informatics, Penanganan Sebaran Konten Hoaks Covid-19 Kamis, (20 January 2022), available at: <https://www.kominfo.go.id/content/detail/39481/penanganan-sebaran-konten-hoaks-covid-19-kamis-20012022/0/infografis>; Media Indonesia, Menkominfo: 767 Hoaks Covid-19 Sudah Ditindak, (23 July 2021), available at: <https://mediaindonesia.com/humaniora/420486/menkominfo-767-hoaks-covid-19-sudah-ditindak>; Neraca, 1.800 Hoaks Ditemukan Kominfo, 767 Kasus Dapat Penindakan Hukum, (27 August 2021), available at: <https://www.neraca.co.id/article/151077/1800-hoaks-ditemukan-kominfo-767-kasus-dapat-penindakan-hukum>
 126. Kyoto Review, The COVID Pandemic and the Evolution of Digital Authoritarianism in Indonesia, (2021), available at: <https://kyotoreview.org/issue-33/the-covid-19-pandemic-and-the-evolution-of-digital-authoritarianism-in-indonesia/>
 127. The Jakarta Post, Epidemiologist Pandu Riono's Twitter account hacked, (20 August 2020), available at: <https://www.thejakartapost.com/news/2020/08/20/epidemiologist-pandu-rionos-twitter-account-hacked.html>
 128. Reuters, Digital attacks raise fears over press freedoms in Indonesia, (24 August 2020), available at: <https://www.reuters.com/article/us-indonesia-media-hacking-idUSKBN25K14G>
 129. SAFEnet, Digital Rights Situation Report Indonesia 2020: Digital Repression Amid the Pandemic, (5 May 2021), available at: <https://safenet.or.id/digital-situation-report-2020/>; CNN Indonesia, Diduga Hina Jokowi soal Corona, Buruh di Kepri Ditangkap, (8 April 2020), available at: https://www.cnnindonesia.com/nasional/20200408192303-12-491818/diduga-hina-jokowi-soal-corona-buruh-di-kepri-ditangkap?utm_source=twitter&utm_medium=oa&utm_content=cnnindonesia&utm_U
 130. Facebook Transparency Report, Content restrictions, (n.d.), available at: <https://transparency.fb.com/data/content-restrictions/country/ID/>
 131. Ministry of Communication and Informatics, [Press Release] Perkembangan Penanganan Hoaks Covid-19 dan PPKM, (25 November 2021), available at: https://kominfo.go.id/content/detail/38332/siaran-pers-no-414hmkominfo112021-tentang-perkembangan-penanganan-hoaks-covid-19-dan-ppkm/0/siaran_pers

132. Tribun News, Kominfo Hapus 5.046 Konten Hoaks Terkait Covid-19 Selama Periode Januari-November 2021, (4 December 2021), available at: <https://www.tribunnews.com/techno/2021/12/04/kominfo-hapus-5046-konten-hoaks-terkait-covid-19-selama-periode-januari-november-2021> (reporting 5,046 identified COVID-19-related hoaxes from January to November 2021); Ministry of Communication and Informatics, Penanganan Sebaran Konten Hoaks Covid-19 Senin (29/11/2021), (29 November 2021), available at: <https://www.kominfo.go.id/content/detail/38382/penanganan-sebaran-konten-hoaks-covid-19-senin-29112021/0/infografis> (reporting 5,178 cases from January 2020 to November 2021 under consideration for access blocking/content takedown).
133. USAID, Technology Facilitated Gender Based Violence in Asia: Indonesia, (2022), available at https://pdf.usaid.gov/pdf_docs/PA00Z77G.pdf
134. International Commission of Jurists, Silenced But Not Silent: Lesbian, Gay, Bisexual and Transgender Persons' Freedom of Expression and Information Online in Southeast Asia, (July 2023), available at <https://icj2.wpenginepowered.com/wp-content/uploads/2023/07/ICJ-Silenced-But-Not-Silent-Report.pdf>
135. Front Line Defenders, Threats And Attacks Against Woman Human Rights Defender Veronica Koman's Family, (11 November 2021), available at: <https://www.frontlinedefenders.org/en/case/threats-and-attacks-against-woman-human-rights-defender-veronica-koman%E2%80%99s-family>; The Guardian, 'It opened my eyes': the Indonesian woman fighting for West Papuan rights, (29 April 2019), available at: <https://www.theguardian.com/world/2019/apr/29/it-opened-my-eyes-the-indonesian-woman-fighting-for-west-papuan-independence>; Lawyers for Lawyers, Veronica Koman: defending the West Papuan indigenous people of Indonesia, (9 August 2020), available at: <https://lawyersforlawyers.org/en/25153/>
136. Benar News, Indonesian Lawyer Wanted over Papua Unrest Defiant in Face of Threats, (21 November 2019), available at: <https://www.benarnews.org/english/news/indonesian/Papua-rights-defender-11212019184820.html>
137. Front Line Defenders, Threats And Attacks Against Woman Human Rights Defender Veronica Koman's Family, (11 November 2021), available at: <https://www.frontlinedefenders.org/en/case/threats-and-attacks-against-woman-human-rights-defender-veronica-koman%E2%80%99s-family>
138. Office of the High Commissioner for Human Rights (OHCHR), Indonesia: Stop reprisals against woman human rights defender – UN expert, (15 December 2021), available at: <https://www.ohchr.org/en/press-releases/2021/12/indonesia-stop-reprisals-against-woman-human-rights-defender-un-expert>
139. Front Line Defenders, Threats And Attacks Against Woman Human Rights Defender Veronica Koman's Family, (11 November 2021), available at: <https://www.frontlinedefenders.org/en/case/threats-and-attacks-against-woman-human-rights-defender-veronica-koman%E2%80%99s-family>
140. Alia Yofira & Dewi Ni Putu Candra, Harapan Menghidupkan Perjuangan: Bergerak Bersama Meretas KBGO in Di Babak Pertama, Semua Berharga, Reflection of First Year Task Force KBGO, (May 2022), available at: bit.ly/catatan-perjalanan
141. Shevierra Danmadiyah, Laporan Aduan Task Force KBGO 2022 in Menata Irama di Jalan tak Berima, Reflection of Task Force KBGO in 2022, (July 2023), available at: bit.ly/catatan-perjalanan2022; Konde.co, Riset TaskForce KBGO 2022: Sextortion Jadi Ancaman Paling Serius, (13 October 2023), available at: <https://www.konde.co/2023/10/riset-task-force-kbgo-2022-sextortion-jadi-ancaman-paling-serius/>
142. Asosiasi Penyelenggara Jasa Internet Indonesia, Profil Internet Indonesia 2022, (June 2022), available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiT4oLAlbyEAxXWzgiHHfK-DewQF-noECCcQAQ&url=https%3A%2F%2Fapjii.or.id%2Fdownload_survei%2F2feb5ef7-3f51-487d-86dc-6b7abec2b171&usg=AOv-Vaw0DzKYDVUQ2WaAFxxWFQQXj&opi=89978449
143. Shevierra Danmadiyah, Laporan Aduan Task Force KBGO 2022 in Menata Irama di Jalan tak Berima, Reflection of Task Force KBGO in 2022, (July 2023), available at: bit.ly/catatan-perjalanan2022
144. Shevierra Danmadiyah, Laporan Aduan Task Force KBGO 2022 in Menata Irama di Jalan tak Berima, Reflection of Task Force KBGO in 2022, (July 2023), available at: bit.ly/catatan-perjalanan2022
145. Alia Yofira & Dewi Ni Putu Candra, Harapan Menghidupkan Perjuangan: Bergerak Bersama Meretas KBGO Di Babak Pertama, Semua Berharga, Reflection of First Year Task Force KBGO, (May 2022), available at: bit.ly/catatan-perjalanan
146. Manushya Foundation, Joint Solidarity Statement: Confronting the Influence of Online Hate Campaigns in the Forced Expulsion of Rohingya from Indonesia, (17 January 2024), available at: <https://www.manushyafoundation.org/js-onlinehatecampaign-rohingya>
147. BBC Indonesia, 'Rohingya di Sidoarjo', 'Rohingya minta tanah', 'Menlu Retno usir Rohingya' –

- Bagaimana narasi kebencian dan hoaks bekerja menyudutkan etnis Rohingya?, (2 January 2024), available at: <https://www.bbc.com/indonesia/artikles/c03y7n3k12lo>
148. Modern Diplomacy, Demonization of Rohingya in Indonesia: An Analysis on Social Media Narratives, (30 December 2023), available at: <https://modern-diplomacy.eu/2023/12/30/demonization-of-rohingya-in-indonesia-an-analysis-on-social-media-narratives/>
149. Manushya Foundation, Let's #ProtectRohingya by Understanding the Rohingya Crisis in Indonesia, (19 January 2024), available at: <https://www.manushyafoundation.org/post/let-s-protectrohingya-by-understanding-the-rohingya-crisis-in-indonesia>
150. Al Jazeera English, Indonesia: 1,700 Rohingya refugees arrived in Aceh since November, (9 January 2024), available at: <https://www.youtube.com/watch?v=eJ7esfqMsvo>
151. South China Morning Post, In Indonesia, fake UN accounts spewing anti-refugee hate feed rejection of Rohingya, (22 December 2023), available at: <https://www.scmp.com/week-asia/people/article/3246022/indonesia-fake-un-accounts-spewing-anti-refugee-hate-feed-rejection-rohingya>
152. South China Morning Post, In Indonesia, fake UN accounts spewing anti-refugee hate feed rejection of Rohingya, (22 December 2023), available at: <https://www.scmp.com/week-asia/people/article/3246022/indonesia-fake-un-accounts-spewing-anti-refugee-hate-feed-rejection-rohingya>
153. South China Morning Post, In Indonesia, fake UN accounts spewing anti-refugee hate feed rejection of Rohingya, (22 December 2023), available at: <https://www.scmp.com/week-asia/people/article/3246022/indonesia-fake-un-accounts-spewing-anti-refugee-hate-feed-rejection-rohingya>
154. Manushya Foundation, Joint Solidarity Statement: Confronting the Influence of Online Hate Campaigns in the Forced Expulsion of Rohingya from Indonesia, (17 January 2024), available at: <https://www.manushyafoundation.org/js-onlinehatecampaign-rohingya>
155. U.S. State Department, 2020 Country Reports on Human Rights Practices: Indonesia, (2020), available at: <https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/indonesia/>
156. Indonesian Criminal Code (1982), available at: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=73932; HG.org, Defamation and Privacy Law in Indonesia, available at: <https://www.hg.org/legal-articles/defamation-and-privacy-law-in-indonesia-5913>
157. Law No. 26 of 2000, Section 4, available at: <https://policehumanrightsresources.org/content/uploads/2019/07/Law-26-2000-Act-on-the-Human-Rights-Courts-2000-Eng.pdf?x39143>
158. Protection International, National Human Rights Institutions and the Protection of Human Rights Defenders: Insights from Indonesia and Thailand, (May 2020), available at: <https://www.protectioninternational.org/sites/default/files/policy-brief-nhri-hrd-hub.pdf>
159. Protection International, National Human Rights Institutions and the Protection of Human Rights Defenders: Insights from Indonesia and Thailand, (May 2020), available at: <https://www.protectioninternational.org/sites/default/files/policy-brief-nhri-hrd-hub.pdf>
160. Protection International, National Human Rights Institutions and the Protection of Human Rights Defenders: Insights from Indonesia and Thailand, (May 2020), available at: <https://www.protectioninternational.org/sites/default/files/policy-brief-nhri-hrd-hub.pdf>
161. Law No. 13 of 2006, available at: http://ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=75101&p_country=IDN&p_count=610&p_classification=01&p_classcount=81
162. American University School of International Service, The State of Whistleblower & Journalist Protections Globally: A Customary Legal Analysis of Representative Cases, (May 2015), available at: <https://www.ohchr.org/Documents/Issues/Opinion/Protection/AmericanUniversitySchool.pdf>
163. Law No. 32/2009 on Environmental Protection and Management, available at: <https://leap.unep.org/en/countries/id/national-legislation/law-no-322009-environmental-protection-and-management>; Law No. 18/2013 on the prevention and eradication of Forest Destruction, available at: <https://leap.unep.org/en/countries/id/national-legislation/law-no-182013-prevention-and-eradication-forest-destruction>

#STOPDIGITAL DICTATORSHIP

