ASEAN Regional Coalition to #StopDigitalDictatorship

#StopDigitalDictatorship

Joint Submission to the United Nations High Commissioner for Human Rights

February 2022

HUMAN RIGHTS DUE DILIGENCE, TECH SECTOR RESPONSIBILITIES AND BUSINESS TRANSPARENCY

@manushyafoundation x ivana

ASEAN Regional Coalition to #StopDigitalDictatorship

For more information on this Joint Submission, please contact:

ALTSEAN-Burma Lead: Debbie Stothard
Email: debbie.stot@gmail.com

Cambodian Center for Human Rights (CCHR) Lead: Chak Sopheap
Email: chaksopheap@cchrcambodia.org

ILGA Asia Lead: Henry Koh
Email: henry@ilgaasia.org

Manushya Foundation Lead: Emilie Pradichit
Email: emilie@manushyafoundation.org

Southeast Asia Freedom of Expression Network (SAFEnet) Lead: Damar Juniarto
Email: damarjuniarto@protonmail.com

ASEAN Regional Coalition to #StopDigitalDictatorship

INPUT FOR OHCHR REPORT ON THE APPLICATION OF THE UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS IN THE TECH SECTOR

The digital transformation of societies is in full swing, and unless adequate measures are in place, the negative impacts will follow. The impact of technology on human rights is undeniable, and, for this reason, tech companies must understand how their activities can cause harm and demonstrate they have processes in place to address them. Tech companies have themselves contributed to rights violations by restricting access to information, allowing the spread of hate speech and other types of harmful content, exposing personal information,[1] and developing artificial intelligence systems with discriminatory biases.[2] Nonetheless, especially given the highly specialised nature of their activities and the opaque nature of their developments such as automated decision-making and artificial intelligence, the link between tech companies and human rights abuses can be subtle. For this reason, tech companies must create a safe and ethical online environment for their users, ensuring the respect for human rights takes centre stage in all their operations.

In Southeast Asia, tech companies are compelled to abide by draconian domestic laws. As threats to national security and public order are broadly and vaguely defined, businesses are required to restrict individuals' rights in the sole interest of the government or power group, in violation of international human rights standards.[3] With civic space in Southeast Asia being threatened by the governments, HRDs, journalists and civil society have started to use the internet and social media platforms as a free space to share their opinions and hold governments accountable for their actions. In turn, Governments have responded by misusing laws and policies to crackdown on dissenting voices and punish the sharing of information critical of the government, obliging tech companies to moderate and remove content, facilitate government surveillance, retain and hand over users' data, and collaborate with the authorities to block or disconnect network connections.[4] In addition, hate speech, misinformation, disinformation, incitement to violence, and other content that causes real-world harm have been rampant on social media platforms in recent years. Vulnerable groups such as indigenous peoples, women, ethnic groups, migrants, persons with disabilities, or LGBTIQ+ individuals are most affected by the adverse conduct of tech companies.[5] There is also the additional threat of powerful new actors on the scene – private surveillance companies – which Governments are increasingly hiring to develop insidious technologies for the targeted digital surveillance of HRDs.[6] Their activities are directly at odds with their responsibilities under international human rights standards and the UNGPs, which require companies to ensure robust due diligence to prevent their products being used to violate human rights and to remedy any harms caused by their products. To guarantee tech companies respect human rights, they must ensure a risk-based approach to due diligence which would permit them to more effectively manage their responsibility to respect human rights and to integrate human rights considerations during key milestones in product development. Tech companies must make human rights a core consideration in their policies.

To avoid being found in violation of specific national laws, private companies may closely monitor their users' activities, upon authorities' requests, thereby invading individuals' privacy. Nevertheless, regardless of whether compelled by the State to do so, companies must, in their own agency, carry out their duty to protect and promote human rights.

The ASEAN Regional Coalition to #StopDigitalDictatorship commends the necessity to ensure that approaches to apply UNGPs are aligned with international norms and that human rights assessments are a key component of identifying, preventing, mitigating, and accounting for how companies address human rights impacts. Underlying the crucial role of technologies for the realisation of a multitude of rights, we also note they can exacerbate inequalities, restrictions on freedom of expression and discrimination. With this Submission, we aim to illustrate and share our views on the type of actions that are required or expected to be taken by companies and states to advance the uptake of the UNGPs to the activities of technology companies, by looking at five key areas presented below:

1. Human Rights as an Element of Corporate Governance

To ensure tech companies put human rights first, they have to conduct comprehensive due diligence on all aspects of their business that may affect users' human rights, including by assessing the possible harm that their new potential activities may cause, and to take actions to mitigate these impacts. Additionally, in their human rights due diligence, companies should also cover adverse human rights impacts that government regulations and policies may cause, and effective ways to mitigate any risks posed by them. By doing so, they would be able to prevent and mitigate harms that may arise through States using technology in ways that violate human rights and undertake further evaluation in a timely manner, in the event of identifying such risks. Human rights impact assessments should be conducted on a regular basis to ensure that their activities – including their decisions and practices – do not cause, contribute to, or aggravate human rights violations. Whenever human rights impact assessments are conducted, particular attention should be paid to three of the rights most likely to be affected by companies' conducts: the rights to privacy, freedom of expression and equality/non-discrimination. In addition, clear restrictions on specific uses of products or services which contravene international human rights standards must be specified. The experience of human rights due diligence in other settings should also guide these efforts. This is particularly important when integrating rights-holder perspectives and focusing on vulnerable groups. Conducting such assessments allows companies to identify potential risks and take measures to mitigate them. Moreover, part of their due diligence responsibility is their duty to disclose information with regards to companies' actions to prevent and limit human rights risks.[7] Such information shall be made available and accessible on their websites.

In addition to conducting human rights due diligence, companies' strong commitment to human rights shall be visible through their efforts to strengthen human rights oversight and respect for human rights. Companies should have strong governance and oversight over human rights at all levels of operation, and ensure that the organisation's leadership is accountable for its policies and practices affecting human rights. It is equally important for companies to train their employees on the importance of respecting human rights in every part of their work and on their role to protect them accordingly. Also, as part of their commitment to respect human rights, companies should actively engage with other stakeholders to realise effective responses in addressing human rights risks and impacts in a business context. This includes effective social dialogue with vulnerable individuals and communities, who are at most risk of human rights violations, or with other stakeholders, including civil society and organisations who play an essential role in monitoring State and business practices, in order to further and advocate for the advancement of human rights.

Finally, full respect for human rights can be achieved only if people enjoy the right to seek redress when their rights have been violated by a company, as well as in the case when the company facilitates such violation. For this reason, it is imperative for companies to have clear grievance and remedy mechanisms in place. Clear, rights-respecting, and predictable appeal mechanisms and processes must be provided likewise, in case of users' willingness to appeal content-moderation actions. Clear timeframes must be established for both procedures.

Of note, tech companies in SEA have often failed to implement the UNGPs, as in the case of Facebook that was an instrument to spread hate speech about Rohingya refugees.[8]

2. Transparency on Practices and Measures taken to Ensure the Respect for Human Rights

Transparency should be reflected across a range of areas in the companies' practices: (1) in their terms and conditions; (2) in decisions on content and users accounts restrictions; (3) in policies on prohibited advertising content and prohibited targeting rules, as well as their enforcement; (4) in policies on prohibited content and accounts, as well as on their actions to restrict/censor content; (5) use of algorithms. Companies should make this information public and assist users in comprehending it by demystifying the complex language embodied in such documents.

Whether it is user account restrictions, internet shutdowns, or actions to restrict content, companies are expected to make their policies publicly available, to regularly report on demands received, and disclose the reports along with the extent of compliance. Not only do they have to report on the number of requests, but also explain how they respond to any inappropriate or overbroad request, and eventually push back on any such demand made by governments or third parties.

With regards to the development and use of algorithms and targeted advertising, companies should maximise their transparency on their policies used and the rules that govern them, as well as their efforts to protect human rights and to account for the potential harms. It is fundamental that companies disclose how algorithms are used in their operations. Similarly, companies must clearly specify what types of advertising are permitted and prohibited, as well as how they detect violations and enforce the rules. The use of targeted advertising systems should be evaluated to ensure they do not embed potential discriminatory impacts and other human rights harms.

3. Users' High Control over their Data and Data Associated with Them

Companies must limit the collection of personal information only if it is directly relevant and necessary to achieve a specific purpose, and refrain from retaining it after the purpose is fulfilled. In this light, they have to disclose what user information they collect and how. Additionally, such information should only be used for the purpose for which it was collected or inferred. Since companies also perform big data analytics to make inferences or predictions about users on the basis of the collected information, transparency and user control over data interference are necessary to predict and understand privacy-invasive and non-verifiable interferences.[9] Nevertheless, the sale, use of and exploitation of user data is commonplace in Southeast Asia, and companies must work to limit their collection of personal information.[10]

Users should have high control over their data. This includes having the right to know how to control the information that companies collect, retain, and infer about them. Companies must assist them in this effort, such as by revealing the length of data retention and the extent to which identifiers are removed from stored user information; by assisting users and allowing them to control how their information is used – applicable also to users' information used for targeted advertising and algorithmic system development. As a result, users would be able to request the deletion of specific types of information about them. Last but not least, companies have to be fully transparent about users' information they share and with whom, and refrain from sharing it with third parties without clear consent from the users. Communications' encryption is another pillar for users to have their private and sensitive data protected, enhancing their ability to control the data associated with them; companies should therefore take necessary measures to encrypt user communications by default in order to protect transmissions of their communications. Although tech companies have committed to adhere to the UNGPs, they may face conflict between domestic laws and human rights commitments. Facebook and Google reported a manifold of government requests to access user data.[11]

4. Well-Informed and Educated Users about Potential Risks

Tech companies have access to vast amounts of data about their users, which makes them attractive targets for malicious actors. That is why companies are responsible for providing users with clear, simple, and easy-to-understand information about cybersecurity risks and how they can protect against such risks.[12] This can include publishing materials on phishing attacks prevention, advanced authentication, privacy settings etc.

5. States' Duty to Protect; Regulatory and Policy Responses

When it comes to overall state duties to protect and duties pertaining to access to remedy, states are expected to take a broad approach to managing the human rights and business agenda, primarily by being aware of business-related human rights risks.

State authorities can use a variety of approaches to support the enactment and implementation of relevant measures related to human rights and business. They can (1) support activities that identify pressing human rights and business issues, high-risk activities and vulnerable groups; (2) increase awareness on human rights and business issues within relevant ministries and agencies of the state; (3) strengthen and support work on human rights and business at international level. States should also consider adopting policies that seek to foster business respect for human rights and guidance to business enterprises.[13] Although there is a plethora of legislation that governs the potential human rights impact of corporate organisations' actions, states should consider adopting laws that clearly stipulate what companies must do to respect human rights. This can include requirements for companies to disclose their commitment to human rights statements, or to act in a socially responsible manner. In addition, states ought to develop policies that encourage tech companies to respect human rights, such as corporate social responsibility, human rights and anti-discrimination policies, as well as other policies that encourage businesses to perform human rights due diligence and publicly report on human rights.

As part of their duty to protect against business-related human rights abuse, states must take appropriate steps to ensure that when such abuses occur within their territory and/or jurisdiction, those affected have access to effective remedy. To fulfil their duty to remedy business-related human rights abuses, states must consider the entire range of remedies at their disposal, including sanctions (criminal or administrative), compensation (financial or non-financial), or other alternatives to sanctions, and measures designed to prevent future harm.[14]

Notably, states have to ensure the effectiveness of state-based judicial mechanisms, including by ensuring that there are no legal or procedural obstacles preventing legitimate cases from being brought before courts, and by harmonising aspects of civil and criminal liability relevant to business operations.[15] In terms of non-judicial grievance mechanisms, the National Human Rights Institutions (NHRI) may be given a mandate that allows it to receive and handle complaints relating to corporate abuses or to offer support to individual cases.

RECOMMENDATIONS

We are living in an era of massive digital transformation, which impacts every facet of society, and as technology advances, it poses many challenges to human rights, security, and governance. Tech companies have been able to conduct their activities regardless of international laws and standards, even when those resulted in violations of human rights; as long as they continue to skirt their human rights responsibilities, human rights violations will increase. While tech companies are accountable to ensure that advances in technology benefit all people and do not exacerbate inequality for marginalised people and vulnerable groups, their action alone will not suffice. To ensure human rights respect and protection, the challenge is to establish a multi-stakeholder collaboration, dialogue, and action to accelerate a truly inclusive approach to ensure that the benefits of digital technology are spread to people around the globe, and not against them.

The ASEAN Regional Coalition to #StopDigitalDictatorship makes the following recommendations to tech companies to advance the uptake of the UNGPs in their industry:

1. Ensure their terms of service and policies are uniform and comply with international standards on freedom of expression and protection of data privacy, 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 UNGPs;
2. Review internal existing policy framework to ensure that they set out a suitably robust position in relation to human rights risks, is endorsed and supported by senior management and is appropriately understood and implemented, particularly by those in the companies who are likely to be closest to human rights risks;
3. Understand the complexities of the countries where they invest, examine the suppliers they buy from, and take into consideration the potential for impact associated with operating in countries where governance is weak and the rule of law is fragile;
4. Ensure that any requests, orders and commands to access information or 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;
5. Conduct assessments and due diligence processes to determine the impact of business activities on users, with respect to online freedom, privacy and data security; Ensure that full participation by and consultation of affected individuals are meaningful, and the results of human rights impact assessments and public consultations are made public;
6. Publish regular information on the official websites regarding the legal basis of requests made by governments and other third parties and regarding the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own policies and community guidelines;
7. Provide company-level remedies and grievance redressal mechanisms both physical and virtual, to victims affected by adverse impacts of cybersecurity responses that violate their rights; Provide users with an opportunity to challenge decisions, particularly on the takedown of or access to their information when unlawful under national or international law; or if the restrictions are unfair and unduly restrictive.

ENDNOTES

[1] OHCHR, *Statement by United Nations High Commissioner for Human Rights, Michelle Bachelet at the 13th Session of the Forum on Minority Issues: Hate speech, social media and minorities*, (November 2020), available at: https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=26519&LangID=E; OECD Watch, *Rohingya refugees supported by Victim Advocates International vs. Facebook*, (9 December 2021), available at: https://www.oecdwatch.org/complaint/rohingya-refugees-vs-facebook/; Time, *Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy*, (29 July 2020), available at: https://time.com/5872868/big-tech-regulated-here-is-4-ways/

[2] Coconet, *Artificial Intelligence and Human Rights: Notes from Coconet II*, (20 December 2019), available at: https://coconet.social/2019/artificial-intelligence-human-rights-coconet/

[3] ICJ, *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia*, (December 2019), available at: https://www.icj.org/wp-content/uploads/2019/12/Southeast-Asia-Dictating-the-Internet-Publications-Reports-Thematic-reports-2019-ENG.pdf

[4] CSIS, *Controlling the Information Space: Big Tech and Free Speech in Southeast Asia*, (26 July 2021), available at: https://www.csis.org/blogs/new-perspectives-asia/controlling-information-space-big-tech-and-free-speech-southeast-asia; Freedom House, *Freedom on the Net 2021 - The Global Drive to Control Big Tech*, (2021), available at: https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech; Manushya Foundation, *Digital Rights in Thailand: Joint Submission to The UN Universal Periodic Review (UPR) for Thailand's third UPR Cycle, 39th session of the UPR Working Group*, (25 march 2021), available at: https://www.manushyafoundation.org/digital-rights-joint-upr-submission

[5] World Economic Forum, *Why tech needs to focus on the needs of marginalized groups*, (8 July 2021), available at: https://www.weforum.org/agenda/2021/07/tech-focus-needs-marginalized-groups/; Digital Freedom Fund, *How Artificial Intelligence Impacts Marginalised Groups*, (29 May 2021), available at: https://digitalfreedomfund.org/how-artificial-intelligence-impacts-marginalised-groups/; ILGA, *Hate Speech on Social Media Is Forcing LGBTI People Back Into Silence. It's Time to Take Action*, (19 March 2021), available at: https://ilga.org/hate-speech-social-media-forcing-lgbti-back-silence-take-action

[6] Amnesty International, *A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work*, (16 August 2019), available at: https://www.amnesty.org/en/latest/research/2019/08/a-dangerous-alliance-governments-collaborate-with-surveillance-companies-to-shrink-the-space-for-human-rights-work/; The Citizen Lab, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, (18 September 2018), available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Reuters, *Apple warns Thai activists "state-sponsored attackers" may have targeted iPhones*, (25 November 2021), available at: https://www.reuters.com/technology/apple-warns-thai-activists-state-sponsored-attackers-may-have-targeted-iphones-2021-11-24/

[7] ASSER Institute, *The Norwegian Transparency Act 2021 – An important step towards human rights responsibilities for corporations*, (29 June 2021), available at: https://www.asser.nl/DoingBusinessRight/Blog/post/the-norwegian-transparency-act-2021-an-important-step-towards-human-rights-responsibilities-for-corporations-by-nora-kenan

[8] Facebook has become the poster company for inaction and lack of due diligence due to the unchecked negative effects Facebook's algorithms and platform have had on human rights. A glaring example of this has been the closely documented case of Facebook contributing to the spread of hate speech and violence against the Rohingya in Myanmar. Widely reported, Facebook's algorithms contributed to proliferation and hate speech in Myanmar that exacerbated violence against Rohingya in the country that has persisted for decades. This stretch of violence has been labelled as a genocide by many accounts and has led to two large-scale exoduses of Rohingya refugees out of Myanmar. *See*: UNHCR, *Rohingya Emergency*, available at: https://www.unhcr.org/rohingya-emergency.html

[9] Ranking Digital Rights, *2020 Indicators*, available at: https://rankingdigitalrights.org/2020-indicators/

[10] This is often a tall order considering many technology companies have their business models centred around the collection and use of collected personal data. Non-vital information collection has a plethora of data leaks and intrusions into privacy. For instance, in Malaysia alone, there have been several data breach instances that underscore concern over user data collection. In 2021, E-pay Malaysia, the largest prepaid top-up and bill collection network, was reportedly leaked, compromising the personal details of at least 380,000 customers that were allegedly sold online. Another such incident led to personal information of over 11 million Malaysian Facebook users including their phone number, full name, birthday, account creation date, relationship status, and bio was leaked online. *See*: KrAsia, *E-pay Malaysia users allegedly affected by data leak*, (5 February 2021), available at: https://kr-asia.com/e-pay-malaysia-users-allegedly-affected-by-data-leak; The Star, *Investigations underway on alleged E-pay data leak, says GHL Group*, (4 February 2021), available at: https://www.thestar.com.my/tech/tech-news/2021/02/04/investigations-underway-on-alleged-e-pay-data-leak-says-ghl-group; Lowyat.net, *Personal Data Of More Than 11 Million Malaysian Facebook Users Leaked Online*, (4 April 2021), available at: https://www.lowyat.net/2021/236599/personal-data-11million-malaysian-facebook-users-leaked/

[11] Facebook Transparency, *Government Requests for User Data*, available at: https://transparency.fb.com/data/government-data-requests/; Google Transparency Report, *Global requests for user information*, available at: https://transparencyreport.google.com/user-data/overview

[12] In instances where user data is compromised, companies need to ensure users are adequately informed on the manner their data has been violated and how they can protect themselves in the future. Throughout 2020 and 2021, numerous cases of data breaches were registered in Southeast Asian countries. In Indonesia, three incidents were reported in May 2020, involving millions of users. Indonesian e-commerce Tokopedia suffered a massive data breach after hackers reported over 15 million user records. It was also discovered that the data of 91 million users was up for sale on the Darknet for US$ 5,000. Despite such instances, countries like Laos, have yet to implement mandatory reporting laws regarding data breaches. Hence, companies must take responsibility to ensure the security of their users' data and that they are promptly and adequately informed about potential risks. *See*: Cisomag, *Tokopedia Data Breach: Hackers Leaks 15 Mn User Records*, (5 May 2020), available at: https://cisomag.eccouncil.org/tokopedia-data-breach-hackers-leaks-15-mn-user-records/; Comparitech, *Database containing personal info of 106 million international visitors to Thailand was exposed online*, (20 September 2021), available at: https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/

[13] Stephanie Lagoutte, The State Duty to Protect Against Business-Related Human Rights Abuses. Unpacking Pillar 1 and 3 of the UN Guiding Principles on Human Rights and Business, *Matters of concern Human rights' research papers Series No. 2014/1*, (16 September 2014), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496355

[14] Stephanie Lagoutte, The State Duty to Protect Against Business-Related Human Rights Abuses. Unpacking Pillar 1 and 3 of the UN Guiding Principles on Human Rights and Business, *Matters of concern Human rights' research papers Series No. 2014/1*, (16 September 2014), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496355

[15] OHCHR, *Corporate liability for gross human rights abuses. Towards a fairer and more effective system of domestic law remedies, A report prepared for the Office of the UN High Commissioner for Human Rights*, (2014), available at: https://www.ohchr.org/Documents/Issues/Business/DomesticLawRemedies/StudyDomesticeLawRemedies.pdf

About ALTSEAN-Burma

ALTSEAN-Burma was formed in October 1996 by a diverse network of organizations and individuals at the Alternative ASEAN Meeting on Burma, held in Bangkok. Their mission is to develop and strengthen strategic relationships among key networks and organizations from Burma, Southeast Asia, and the international community; support cooperation and partnership among activists, particularly women, youth, ethnic groups, LGBTQ+, displaced people, migrants, and other marginalized communities; implement innovative strategies that are responsive to emerging needs and urgent developments; and produce practical resources for these purposes. ALTSEAN has pursued its mission through advocacy, training and collaboration, focusing on women's participation and leadership, business and human rights, atrocity prevention, and broader human rights and democracy issues. ALTSEAN supports grassroots activists by ensuring local voices are heard at international strategy forums, including their robust analysis and policy recommendations.

About Cambodian Center for Human Rights

CCHR is a leading non-aligned, independent, non-governmental organization that works to promote and protect democracy and respect for human rights – primarily civil and political rights - in Cambodia. It empowers civil society to claim its rights and drive for progress; and through detailed research and analysis it develops innovative policy, and advocates for its implementation.

About Foundation for Media Alternatives

Founded in 1987, the Foundation for Media Alternatives (FMA) assists citizens and communities, especially civil society organizations (CSOs) and other disadvantaged sectors, in the strategic and appropriate use of information and communications technologies (ICTs) for democratization and popular empowerment. FMA exists to enable the empowerment of civil society and social movements in the information age by advocating for democratic governance of ICTs; human rights in digital environments; equitable and safe access to and responsible use of ICTs; gender-transformative perspectives, policies and practices – through critical and meaningful engagement with development stakeholders.

About ILGA Asia

ILGA Asia is the Asian Region of the International Lesbian, Gay, Bisexual, Trans, and Intersex Association, representing more than 190 member organisations across East Asia, South Asia, Southeast Asia, and West Asia. Our vision is a world where Asia is a safe place for all, where all can live in freedom and equality, be properly informed in the nature of sexual orientation and gender identity & expression and sex characteristic (SOGIESC) rights, have access to justice, and diversity is respected.

About Institute for Policy Research and Advocacy (ELSAM)

The Institute for Policy Research and Advocacy (ELSAM) is a civil society organisation that works to enhance the democratic political order in Indonesia by empowering civil society. Founded in 1993, it actively participates in efforts to promote human rights through policy and legal research, advocacy, and training.

About Manushya Foundation

Manushya Foundation was founded in 2017 with the vision to build a movement of Equal Human Beings *#WeAreManushyan.* Manushya is an intersectional feminist human rights organization reinforcing the power of humans, in particular women, human rights defenders, indigenous peoples, forest-dependent communities, environmental defenders, LGBTI groups, and Youth, to be at the heart of decision-making processes that concern them and to speak truth to power at the forefront of their fight for Human Rights, Equality, Social Justice and Peace. Through coalition building, capacity building, community-led research, advocacy and campaigning, and sub-granting, local communities become Agents of Change fighting for their rights and providing solutions to improve their lives and livelihoods, pushing back on authoritarian governments and harmful corporations. Manushya defends local communities and seeks justice with them before the United Nations, focusing on women's rights and gender equality, digital rights, climate & environmental justice, and corporate accountability across Asia.

About Southeast Asia Freedom of Expression Network (SAFEnet)

SAFEnet is a network of digital rights defenders in Southeast Asia which was established on 27 June 2013 in Bali, Indonesia. The establishment of SAFEnet was motivated by the widespread criminalization of netizens because of its expression on the Internet after the enactment of Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). This prompted a number of bloggers, journalists, Internet governance experts, and activists to form this association. In 2018, SAFEnet began to widen the issue of advocacy towards the fulfilment of digital rights after previously only focusing on advocating freedom of expression on the Internet.

About Women's Peace Network

Women's Peace Network is composed of lawyers, community leaders, and peace activists from Myanmar and around the globe who share a common goal: peacefully promote and protect human rights. They strive to ensure that Myanmar is a place where all people can enjoy peace, justice, and prosperity and live together harmoniously.They work to protect the rights, enhance the status, and increase the inclusion of marginalized women, youth, and communities in the Rakhine state and across Myanmar, so that they can live peacefully and prosperously.

ASEAN Regional Coalition to #StopDigitalDictatorship

Cambodian Center for Human Rights · ELSAM · SAFEnet · MANUSHYA #WeAreManushyan ∞ Equal Human Beings · ALTSEAN BURMA SINCE 1996 · Women Peace Network · Foundation for Media Alternatives · ILGA ASIA

MANUSHYA
#WeAreManushyan ∞ Equal Human Beings

Contact us at:
WeAreManushyan@manushyafoundation.org
www.manushyafoundation.org

@manushyafoundation @ManushyaFdn Manushya Foundation