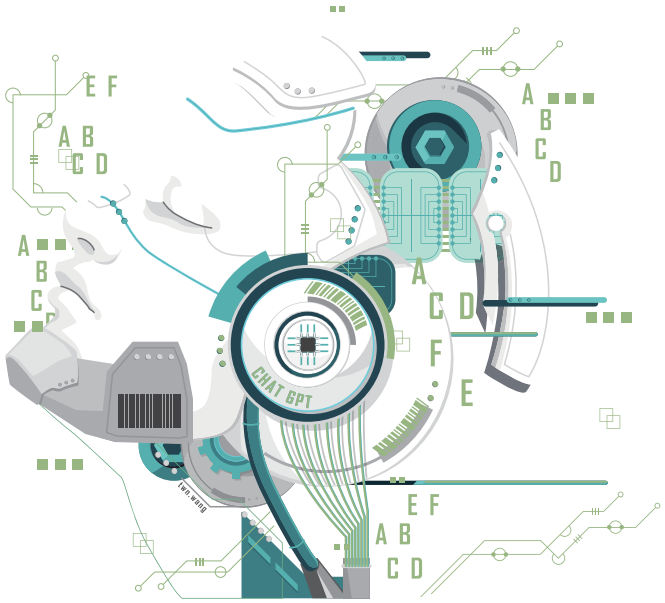
Emerging Technologies and Human Rights

Volume 6 Human Rights and Peace Textbook Series

Edited by
Ratnaria Binti Wahid and Kalpalata Dutta



Supported by

ASEAN University Network
Human Rights Education (AUN-HRE)

Institute of Human Rights and Peace Studies
Mahidol University

UiO : Norwegian Centre for Human Rights
University of Oslo

Emerging Technologies and Human Rights

Volume 6, Human Rights and Peace Textbook Series

By

ASEAN University Network - Human Rights Education and Institute of Human Rights and Peace Studies, Mahidol University

With the support of the Norwegian Centre for Human Rights, University of Oslo

Edited by
Ratnaria Binti Wahid and Kalpalata Dutta

Emerging Technologies and Human Rights

Volume 6, Human Rights and Peace Textbook Series

ISBN: 978-616-622-098-8
ISBN E-Book: 978-616-622-099-5

Published by
Institute of Human Rights and Peace Studies, Mahidol University

Printed by
Scand-Media Corp. Ltd, Bangkok, Thailand

With support of
Norwegian Centre for Human Rights, University of Oslo

AUN-HRE Secretariat
Institute of Human Rights and Peace Studies (IHRP)
Mahidol University
999 Phuttamonthon 4 Road, Salaya,
Nakon Pathom 73170, Thailand

Preface

In response to requests from its network members, ASEAN University Network - Human Rights Education (AUN-HRE) organised a meeting on the theme of "Human Rights and Emerging Technologies" in 2022. The 4-day online meeting brought together lecturers and practitioners from Southeast Asia to discuss emerging technologies, their significance, and their implications for human rights. The discussions during the meeting highlighted the need to examine the subject in greater detail; accordingly, it was decided to compile a textbook on the theme of "Emerging Technologies and Human Rights." Dr Ratnaria Binti Wahid, one of the facilitators of the online workshop, gladly assumed responsibility for leading the compilation and editing of the textbook. Dr Kalpalata Dutta agreed to be a co-editor.

The textbook on Emerging Technologies and Human Rights is the sixth volume in AUN-HRE's series of textbooks on human rights and peace. The textbook is divided into eight chapters:

> Chapter 1, authored by Dr Ratnaria Binti Wahid, lays the foundations by providing an overview of emerging technologies and the human rights framework. It also discusses some of the positive and negative impacts of emerging technologies on the enjoyment of human rights.
>
> Chapter 2, authored by Dr Ratnaria Binti Wahid, examines the international standards, national laws, and ASEAN-level standards and policies that address human rights in the digital realm, specifically with regard to data protection, cybersecurity, and artificial intelligence.
>
> Chapter 3, authored by Dr Azizi Ab Aziz, strengthens critical understanding of artificial intelligence (AI), the various AI learning mechanisms and principles, and the frameworks governing responsible AI.
>
> Chapter 4, co-authored by Dr Kalpalata Dutta and Dr Ratnaria Binti Wahid, examines digital citizenship and the dynamics of citizenship rights in the digital environment. Specifically, it examines digital identity systems; the exercise of the right to vote and participation in public affairs in the digital environment; the use of emerging technologies by courts, law enforcement, and surveillance; and the implications of these developments for human rights.
>
> Chapter 5, authored by Dr Patricia Rinwigati Waagstein, discusses the impact of automation on labour and human rights. Broadly, it discusses the reshaping of labour in the era of technology, its impact on human rights, and the corresponding obligations of State and non-state actors.
>
> Chapter 6, co-authored by Dr Md. Zahurul Haq, Dr Ratnaria Binti Wahid, and Dr Kalpalata Dutta provides a critical overview of environmental technologies and their impact on human rights. Specifically, it discusses the scope of the right to a healthy environment, the concepts of corporate accountability and FPIC for Indigenous peoples, and existing frameworks for addressing climate change. It further critically examines some environmental technologies and their applications in ASEAN.
>
> Chapter 7, authored by Dr Chomkate Ngamkaiwan, analyses the digital divide in Southeast Asia, examining dimensions such as skills, affordability, and structural gaps. It also provides an understanding of the human rights-based approach (HRBA) to digital inclusion by examining the different spheres of digital rights against the core principles of HRBA.
>
> Chapter 8, the last chapter, authored by Dr Azizi Ab Aziz, examines the governance framework needed for emerging technologies and the challenges in developing such a framework.

Dr Mike Hayes at the Institute of Human Rights and Peace Studies, Mahidol University reviewed all the chapters and helped the editors in making the difficult and sometimes overly technical subject of emerging technologies relatable to students of human rights. Consequently, case studies from Southeast Asia, questions for reflection and discussion, human rights insights, and "You Are Here" blurbs were added wherever needed. Frameworks and issues such as the UN Guiding Principles on Business and Human Rights, State Obligations, and Data Protection are common to all the human rights themes. In this regard, the editors have sought to provide a broad understanding of these frameworks in the introductory chapters, whereas the later chapters focus on the specifics of the theme. For example, while the first chapter provides a general understanding of State obligations and the obligations of non-state actors, such as corporations, chapter five discusses state and corporate obligations specifically with respect to the right to work. References used in the different chapters are provided as "Further Reading". Care has been taken to include readings that are freely and easily available, so that all students can access them without difficulty. We hope that students find this textbook useful in forming a critical understanding of emerging technologies and their impact on human rights.

We sincerely acknowledge the efforts of all the authors and editors in compiling the textbook. We especially thank Dr Mike Hayes, who agreed to review the textbook despite his busy schedule. Lastly, we acknowledge the continued support of the Norwegian Centre for Human Rights in the production of learning resources.

AUN-HRE Secretariat
January 2026

Human Rights and Peace Textbook Series

Volume 1, First Edition 2015 **Reprint, 2017**	**An Introduction to Human Rights in Southeast Asia - Volume 1** Edited by Azmi Sharom, Hadi Rahmat Purnama, Matthew Mullen, Melizel Asuncion and Michael (Mike) Hayes; Published by Southeast Asian Human Rights Studies Network (SEAHRN); Supported by Swedish International Development Cooperation Agency (SIDA) *The first edition has been translated in Khmer, Myanmar and Thai languages.*
Volume 2, First Edition 2016 **Reprint, 2017**	**An Introduction to Human Rights in Southeast Asia - Volume 2** Edited by Ayesah Uy Abubakar, Azmi Sharom, Matthew Mullen, Melizel Asuncion, Michael (Mike) Hayes; Thi Tanh Hai Nguyen and Yanuar Sumarian; Published by Strengthening Human Rights and Peace Research and Education in ASEAN / Southeast Asia (SHAPE-SEA); Supported by Swedish International Development Cooperation Agency (SIDA) and Norwegian Centre for Human Rights (NCHR), University of Oslo. *The second edition has been translated to Myanmar language.*
Volume 3, First Edition 2019	**Introduction to Human Rights in Southeast Asia - Volume 3** Edited by Michael (Mike) Hayes, Sriprapha Petcharamesree and Kalpalata Dutta Published by Strengthening Human Rights and Peace Research and Education in ASEAN/Southeast Asia (SHAPE-SEA) and ASEAN University Network - Human Rights Education (AUN-HRE) Supported by the Norwegian Centre for Human Rights (NCHR), University of Oslo *The volume 3 has been translated to Myanmar language.*
Teaching Manual on Human Rights	Published by ASEAN University Network - Human Rights Education (AUN-HRE) and Strengthening Human Rights and Peace Research and Education in ASEAN / Southeast Asia (SHAPE-SEA) Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo

Volume 4, 2021	**Peace and Conflict Transformation in Southeast Asia - A Sourcebook** Edited by Kamarulzaman Askandar Published by ASEAN University Network - Human Rights Education (AUN-HRE), Strengthening Human Rights and Peace Research and Education in ASEAN / Southeast Asia (SHAPE-SEA) and Southeast Asian Conflict Studies Network (SEACSN) Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo
Volume 1, Revised Second Edition 2024	**An Introduction to Human Rights in Southeast Asia - Volume 1** Edited by Vachararutai Boontinand and Kalpalata Dutta Published by ASEAN University Network - Human Rights Education (AUN-HRE) and Institute of Human Rights and Peace Studies (IHRP), Mahidol University Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo
Volume 2, Revised Second Edition, 2024	**An Introduction to Human Rights in Southeast Asia - Volume 2** Edited by Kalpalata Dutta and Vachararutai Boontinand Published by ASEAN University Network - Human Rights Education (AUN-HRE) and Institute of Human Rights and Peace Studies (IHRP), Mahidol Universit Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo
Volume 5, 2024	**Human Rights, the Environment and Climate Change** Edited by Azmi Sharon, Sriprapha Petcharamesree and Kalpalata Dutta Published by ASEAN University Network - Human Rights Education (AUN-HRE) and Institute of Human Rights and Peace Studies (IHRP), Mahidol University Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo
Volume 6, 2026	**Emerging Technologies and Human Rights** Edited by Ratnaria Binti Wahid and Kalpalata Dutta Published by ASEAN University Network - Human Rights Education (AUN-HRE) and Institute of Human Rights and Peace Studies (IHRP), Mahidol University Supported by Norwegian Centre for Human Rights (NCHR), University of Oslo

Emerging Technologies and Human Rights

Volume 6 in Human Rights and Peace Textbook Series

Authors

Azizi Ab Aziz (PhD), STEM (Science, Technology, Engineering & Mathematics) Academy, College of Arts and Sciences, Universiti Utara Malaysia, Malaysia

Chomkate Ngamkaiwan (PhD), Institute of Human Rights and Peace Studies, Mahidol University, Thailand

Kalpalata Dutta (PhD), ASEAN University Network - Human Rights Education

Patricia Rinwigati Waagstein (PhD), Faculty of Law, Universitas Indonesia, Indonesia

Ratnaria Binti Wahid (PhD), College of Law, Government and International Studies, Universiti Utara Malaysia, Malaysia

Md. Zahurul Haq (PhD), Department of Law, Eastern University, Bangladesh

Reviewer

Michael (Mike) Hayes (PhD), Institute of Human Rights and Peace Studies, Mahidol University, Thailand

Editors

Ratnaria Binti Wahid (PhD), College of Law, Government and International Studies, Universiti Utara Malaysia, Malaysia

Kalpalata Dutta (PhD), ASEAN University Network - Human Rights Education

Project Team

The project was coordinated by the AUN-HRE Secretariat team of Vachararutai Boontinand, Kalpalata Dutta and Teetach Kraisornthanaphon

Contents

Chapter 1:

Introduction to Technology and Human Rights

Reader's Guide

This opening chapter invites you to see technology not as something neutral, but as a powerful force that can both expand and threaten human rights in everyday life. From the apps you use to call a Grab ride, scroll through TikTok, or send money through GCash, to the facial-recognition cameras in malls and the algorithms that decide what you see online, technology is reshaping how we live, work, and connect. In this chapter, you will discover why the same tools that give us freedom and opportunity can also enable surveillance, deepen inequality, or spread harmful disinformation. By the end, you will have the foundation to ask critical questions and imagine solutions that put human dignity first. In this chapter, you will:

- Unpack the two faces of technology: a source of empowerment and a potential threat to rights.
- Unpack the human rights framework.
- See how technology can promote justice, inclusion, and voice, especially for marginalised communities.
- Recognise the most common harms (privacy invasion, bias, censorship, misinformation) and why they matter to you and your society.

Start thinking about your own role in shaping technology and its applications so that it respects everyone's rights. Let's begin.

Key Terms

- **Technology:** Any new scientific advancement which has a practical purpose and which impacts society. The technology comes in many forms, for example, it may be digital (about the internet and management of information), it may be engineering (the invention of drones) or bio-medical (the use of genetic engineering).

You Are Here: You Didn't Choose This Pace

You were born into a world where technology changes faster than laws, schools, and social norms. You didn't choose facial recognition, AI systems, or constant connectivity, but you live with their consequences every day.

1.1 Technologies Changing Societies

At its core, technology is the collection of information and the instruments used to reach specific goals. Many basic tools rely on simple scientific principles. For example, the wheel acts like a rotating lever to move force in a circle, while transportation engines rely on the principle that petrol expands when heated. Manipulation of waves underlies many systems: light waves in cameras, sound waves in microphones, and radio waves in telecommunications.

Emerging technologies increasingly rely on binary numbers and algorithms. The binary system uses sequences of binary digits (bits) to represent and digitise things like light, sound, and touch, while algorithms are structured instructions that allow everything from simple calculators to powerful computers to function. Let us have a look at some of the advanced technologies that make up our world today. These new ideas do not stand alone; they build on one another, creating a network of fast progress and new social dynamics.

1.1.1 Artificial Intelligence (AI) and Automation

Artificial Intelligence (AI) is the "brain" of modern technologies. It refers to systems that utilise digital algorithms to perform tasks that once required human intellect, such as understanding speech, analysing images, or making predictions. People use AI every day; it underpins recommendation engines that suggest movies on Netflix, filters that identify spam in our inboxes, and virtual assistants like Siri that respond to voice commands. Besides these daily conveniences, AI is also used in professional fields. In medicine, it assists doctors in diagnosis by spotting patterns in medical scans and in finance, it helps bankers detect fraudulent transactions. However, since algorithms are trained on historical data, they can inadvertently learn and automate human biases, raising human rights concerns.

1.1.2 The Internet of Things (IoT) and Big Data

While AI is like the brain, the Internet of Things (IoT) is like the nervous system of the digital age. Through sensors, IoT connects everyday devices like phones, watches, and industrial machinery to the Internet. This constant connectivity creates "Big Data," a digital exhaust of human behaviour often gathered without the user's explicit knowledge. This technology drives surveillance capitalism, where personal data is turned into products designed to anticipate and influence how people act.

1.1.3 Blockchain and Decentralised Systems

Blockchain, originally developed to power cryptocurrencies like Bitcoin, records transactions in a way that makes tampering or hacking difficult. But its potential goes far beyond finance; it also provides secure, transparent solutions for supply chain management, digital identity systems, and official records such as land ownership. In this way, blockchain replaces reliance on centralised institutions such as state agencies or banks with reliance on decentralised networks and transparent code. However, this shift also raises a critical question: if a decentralised system fails or causes injustice, who is to be held accountable?

1.1.4 Autonomous and Intelligent Systems

We are entering an era in which machines such as delivery drones, self-driving cars, and unmanned military aircraft operate in the physical world without human supervision. Unlike standard AI, these systems possess physical agency. Drones and military robots are now used in armed combat. While this may make it safer for soldiers, robots can pose greater dangers to civilians, especially if they use AI to locate and attack targets.

1.1.5 Immersive, Biological, and Quantum Frontiers

Immersive technologies such as VR and AR (virtual and augmented reality) bring the digital and physical worlds together, changing the way we study, train, and interact. Think of how medical students may practise surgery in a simulated setting or how museums could offer virtual tours that feel real. Wearables and biotechnology are changing how we monitor our health. Finally, quantum computing promises to process information at speeds hard to imagine, potentially solving challenges in encryption, logistics, and drug development that current computers cannot.

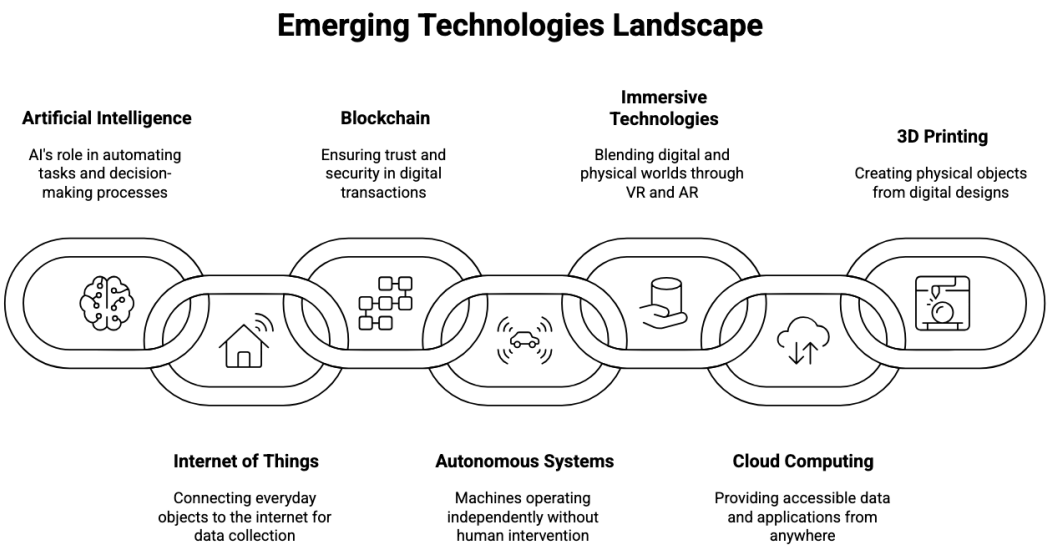
1.1.6 Cloud Computing, Cybersecurity, and Robotics

Every digital invention depends on invisible infrastructure. Cloud computing allows global collaboration by hosting data on remote servers, while cybersecurity acts as the lock and alarm system for our digital lives. These tools ensure that as we move toward 3D printing (turning digital designs into physical objects) and robotics, the underlying systems remain stable and protected from malicious interference.

1.1.7 Nuclear Applications

Some technologies remain vital due to their unique physical properties. Despite the controversies surrounding it, nuclear technology remains an essential pillar for carbon-free electricity, medical radiation therapy, and industrial sterilisation.

Figure 1.1: Emerging Technologies Landscape



All these technologies do not operate in silos. AI makes IoT work better, Big Data gives AI more information, blockchain protects data transactions, and cloud computing stores and shares everything. They all work together to create an ecosystem of innovation that is constantly changing, connected, and dynamic. But this interconnectedness also increases risks: cybersecurity breaches, privacy violations, and the widening gap between people with digital access and those without. As Southeast Asia adopts digital technology, the digital divide between rural and urban areas, as well as between the rich and the poor, becomes a major human rights concern of our time. Figure 1.1 shows the emerging technological landscape. Table 1.1 further outlines several categories of modern technologies, each with unique applications and implications.

Table 1.1: Modern Technologies and Their Applications

Category	Description	Examples/Applications
Artificial Intelligence (AI)	Technology enabling machines to simulate human intelligence.	Natural Language Processing (e.g., chatbots), computer vision generative AI, predictive analytics.
Internet of Things (IoT)	A network of interconnected devices exchanging data through sensors and software.	Smart homes, industrial automation, health monitoring.
Blockchain	Decentralized ledger system ensuring secure and transparent transactions.	Cryptocurrencies, supply chain management, digital identity systems.
Cloud Computing	Remote access to data, applications, and services over the internet.	SaaS platforms (cloud based software service), scalable data storage solutions.
Cybersecurity	Technologies for safeguarding systems, networks, and data from threats.	Firewalls, encryption, intrusion detection systems.
Virtual and Augmented Reality (VR/AR)	Immersive technologies blending virtual or digital elements with the real world.	Gaming, virtual training, education, marketing.
Quantum Computing	Computation using quantum-mechanical phenomena for solving complex problems.	Drug discovery, logistics optimization.
Biotechnology	Use of biological systems to create products or processes.	Genetic engineering, medicine, biofuels, vaccine development.
Robotics and Automation	Use of robots and algorithms for tasks traditionally performed by humans.	Drone, Manufacturing, autonomous vehicles, space exploration.
Communication Technology	Tools for transmitting, storing, and managing information.	Internet, satellite systems, mobile networks.
Wearable Technology	Electronic gadgets worn on the body for various purposes.	Smartwatches, fitness trackers, AR goggles.
3D Printing	Technology creating three-dimensional objects from digital models.	Prototyping, healthcare devices, architectural models.
Nuclear Technology	Techniques manipulating atomic nuclei for energy or other applications.	Power plants, medical radiography, sterilization.

Reflection and Discussion

- *Imagine you are a judge in Jakarta. A self-driving Gojek vehicle causes the death of a motorcyclist. Decide who should pay compensation: the passenger, Gojek, the car manufacturer, or the government, and explain why.*
- *You wear a smartwatch that monitors your heartbeat, fitness, sleep patterns, and fertility cycle. Do you know where all the health data is stored and who can access it? Do you believe your personal bodily information remains private once you start wearing a smartwatch?*

The story of emerging technology is not just about progress. It is a story of choice. Ultimately, the goal is not to resist technology but to humanise it. The application of new technologies should aim to enhance human rights, security, sustainability and equity.

1.2 Overview of Rights Framework

Understanding the rights framework involves understanding the range of human rights, the corresponding obligations, and the mechanisms for their implementation.

1.2.1 Overview of Rights

Human rights can be organised into distinct categories, each with unique characteristics and implications, as outlined in the Universal Declaration of Human Rights (UDHR) 1948 and subsequent international treaties.

Civil and political rights: While many Civil and Political Rights have existed in societies for millennia, they are often associated with the European Enlightenment, which emerged in the 17th and 18th centuries and was shaped by struggles to limit absolute state power. These rights are recognised in the UDHR and the International Covenant on Civil and Political Rights (ICCPR), 1966. **Civil rights** prioritise individual liberty and protection from arbitrary and unjust state interference. Key examples include freedom of expression, religious freedom, the right to property, the rights to life, liberty, and security, rights in the administration of justice, and the right to privacy. **Political rights** are deeply interconnected with civil rights, but serve a different purpose: to recognise political participation. These include the rights to assemble and associate, to participate in the conduct of public affairs, to vote and be elected in free and fair elections, and to access public service. Most civil and political rights are not absolute - in simple terms, ICCPR permits States to draw boundaries to their exercise to protect interests such as national security, public safety, public order, public health, or the rights and freedoms of others. But the States do not have limitless power to draw these boundaries - the rights guarantees in the ICCPR itself lay down the conditions for such boundaries: they must be written into law, have a legitimate purpose, and be necessary and proportionate to that purpose.

Economic, Social and Cultural Rights: Economic, social and cultural rights are recognised in the International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966. **Economic rights** are rights that ensure people can work, earn money, and receive help if they are unable to find employment. These rights emerged strongly in the 20th century, particularly in the aftermath of the Industrial Revolution, where workers' conditions were almost like slavery for many poor people. The ICESCR recognises that workplace rights, such as minimum pay, non-discrimination, and safety, are fundamental to work. **Social rights** are rights that ensure the necessities for a life with human dignity, such as the right to social security, adequate food and water, adequate housing, health, and education. **Cultural rights** protect individuals' and communities' rights to enjoy, practice, and promote their own culture. These rights include the rights to language, art, belief and knowledge systems. Apart from these rights, Article 15 1(b) recognises **the right of everyone to enjoy the benefits of scientific progress and its applications**. Understanding Article 15, together with other rights recognised in the ICESCR, implies that all persons have the right to enjoy the benefits of scientific progress and its applications in the fields of education, healthcare, employment and conditions of employment, housing, food and water security, and the delivery of social security and other public services.

Environmental Rights: Environmental rights safeguard entire communities and future generations by ensuring access to a safe, clean, and sustainable environment. These include rights to clean, pollution-free air and water; rights to healthy, sustainably produced food; rights to healthy ecosystems and biodiversity; and rights to a safe climate. Environmental rights also include protections such as the right to access environmental information, the right to participate in the development of laws and policies relating to the environment and the right to access effective remedies. These different components of environmental rights are recognised in the ICCPR and ICESCR. In contemporary times, as the world experiences the intensifying effects of climate change and countries are facing ecological crises, environmental rights have grown in importance.

Rights of Vulnerable Groups: Certain groups, like indigenous peoples, people with disabilities, migrant workers and their families, require specific protections due to vulnerabilities related to their status or unique circumstances. Specific instruments such as the International Convention on the Elimination of All Forms of Racial Discrimination, the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP, 2007), Convention on the Rights of Persons with Disabilities (CRPD, 2006), and International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (CMW, 1990) addresses these circumstances and specific barriers that impedes the enjoyment of rights.

Digital Rights: As more of our lives move online, whether for school, work, or socialising, the concept of digital rights has emerged to protect our freedoms in the digital world. These rights ensure that the same protections we have in the physical world, such as privacy and free speech, apply online as well. Digital rights can be understood through several primary areas :

1. Traditional Rights in Online Spaces: This refers to the enjoyment and exercise of rights recognised in the ICCPR and ICESCR in online spaces, or through the internet. For example, exercising the right to free speech and expression on social media, or exercising the right to assembly by joining online protests. Much of the work on digital rights focuses here.
2. Data Protection Rights: This area is about keeping the user's personal information safe online so it cannot be used to harm the user. It includes the right to privacy, secure data storage, protection from online surveillance, and the right to be forgotten, which lets you request the deletion of your data.
3. Access to Digital Tools and Services: This area ensures that everyone can use the internet and digital services, such as online education, government websites, and apps. It is about ensuring that everyone has access to the internet, devices, and information, especially in places with limited resources.
4. Participating in Governance of the Digital World: This area is about having a say in how the internet and digital world are run. It includes the right to be involved in decisions about internet policies, ensuring the digital world is fair and inclusive for everyone.

These digital rights are crucial because technology can both empower us and pose risks, such as data theft or censorship. While discussing digital rights, it is worth noting that there are currently no specific international human rights instruments on the subject. Instead, digital rights are anchored in the rights recognised in the UDHR, ICCPR, and ICESCR, collectively known as the International Bill of Rights.

Reflection and Discussion:

In your opinion, should Internet access be recognised as a human right? Why or why not?

An essential principle of human rights is that all persons should be able to enjoy all their rights without distinction of any kind based on race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. This principle of **equality and non-discrimination** is at the core of the human rights framework.

Another principle is that of **interdependence and indivisibility**, meaning that all rights, civil, political, economic, social, and cultural, are connected and equally important. You can imagine human rights as a big colourful puzzle where every piece fits together perfectly. You cannot pick and choose which pieces matter. Every single one is crucial to complete the picture. The Vienna Declaration and Programme of Action 1993, made this clear, stating that all human rights are universal, indivisible, interdependent and interrelated.

While human rights standards set out in the treaties have evolved since their introduction in the UDHR, they have not always kept pace with rapid technological development. From social media to artificial intelligence, technology changes how we live, work, and connect, and sometimes it creates new risks to our freedoms. Luckily, the core ideas of human rights, fairness, dignity, and equality are flexible and can tackle these challenges.

1.2.2 Overview of Obligations

An essential component of rights is obligations or duties - in fact, every right has a corresponding obligation. In the case of human rights, obligations are held by State and non-state actors.

State Obligations: Obligations under ICCPR and ICESCR, while similar at their core, differ slightly in nature. Article 2 of both the ICCPR and ICESCR outlines the nature of State obligations. General Comment No. 31, issued by the Human Rights Committee in 2004, explains the provisions of Article 2 of the ICCPR, while General Comment 3, issued by the Committee on Economic, Social and Cultural Rights in 1990, describes the nature of Article 2 of the ICESCR. Further, the General Comments issued by the Committees on other articles of the Covenants also clarify the nature of obligations under the Covenants.

Article 2, ICCPR	Article 2, ICESCR
1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognsed in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. 2. Where not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognised in the present Covenant. 3. Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognised are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy (c) To ensure that the competent authorities shall enforce such remedies when granted.	1. Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realisation of the rights recognised in the present Covenant by all appropriate means, including particularly the adoption of legislative measures. 2. The States Parties to the present Covenant undertake to guarantee that the rights enunciated in the present Covenant will be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. 3. Developing countries, with due regard to human rights and their national economy, may determine to what extent they would guarantee the economic rights recognized in the present Covenant to non-nationals.

There are some common features of State obligations under ICCPR and ICESCR. They are:

- First, obligations under the covenants apply to all branches of the government (executive, legislative and judicial) and government agencies at all levels - national, regional or local.
- Second, Articles 2(1) and 2(2) of the ICCPR and the ICESCR impose a general obligation on States to ensure that all individuals under their jurisdiction enjoy the rights guaranteed by the ICCPR and the ICESCR, without discrimination. This obligation is immediate, meaning States must comply with it once they have become parties to the Covenants and accepted the obligations under them.
- Third, the phrase “Undertakes to take steps” indicates that States have to consider adopting legislative, judicial, administrative, educational, and other appropriate measures to meet their obligations under the Covenant.
- Fourth, States must respect the rights (also known as the obligation of respect) guaranteed under the Covenants and must refrain from taking any action that violates the enjoyment of the rights.

- Fifth, States must also protect against violations of rights committed by State as well as non-state actors or entities (also known as the obligation to protect). This obligation requires States to take measures to prevent, investigate, punish and provide remedies through effective policies, legislation, regulatons and adjudication.

Apart from these common features, the ICCPR and the ICESCR impose distinct obligations.

Under the ICCPR, the Human Rights Committee, in General Comment 31, has stressed that any restrictions or limitations imposed by States on a right must be permissible under the relevant provisions of the Covenant. Further, when such restrictions are imposed, States must ensure that the measures are prescribed by law, necessary, and proportionate to achieve the stated objectives. Further, the limits imposed must not be such that they diminish entirely the enjoyment of the right recognised under the Covenant. Another component of State obligation under ICCPR is the obligation to provide a remedy as mentioned in Article 2(3) of the Covenant. In this regard, States must ensure that individuals have access to effective remedies to vindicate their rights by establishing appropriate judicial and administrative mechanisms for addressing claims of rights violations.

In contrast, Article 2 of the ICESCR does not explicitly mention the right to effective remedies. Instead, Article 2 (1) of the ICESCR requires States to take appropriate measures, to the maximum of their available resources, with a view to "achieving progressively the full realisation of rights" recognised under the Covenant. This obligation, also known as the obligation of progressive realisation, recognises that States require budgetary resources to achieve the goal of full realisation of the rights recognised under the ICESCR and thus requires them to move towards those goals as expeditiously and effectively as possible. However, it must be noted that not all obligations under the ICESCR are to be progressively realised. The obligation of equality and non-discrimination is immediate, meaning States must provide an effective remedy if they breach it.

In ASEAN, Brunei, Malaysia, Myanmar, and Singapore have not ratified the ICCPR. Brunei, Malaysia and Singapore have not ratified the ICESCR.

Obligations of Non-State actors: Not only do States have obligations to respect human rights guaranteed under international human rights treaties, but non-state actors, such as private entities and individuals, also have obligations. In the context of technology, this category of obligations becomes vital. Businesses have become major actors in developing emerging technologies and their applications, and individuals are significant users of such technologies.

As discussed in the previous paragraphs, under the Covenants, States have the responsibility to protect rights against violations by non-state actors. The Covenants do not elaborate on the measures that non-state actors, such as businesses, should take. Addressing this gap, the **United Nations Guiding Principles on Business and Human Rights (UNGPs)** was endorsed by the Human Rights Council in 2011. These Principles are founded on three pillars: the state's obligation to protect (Pillar 1); businesses' responsibility to respect (Pillar 2), and the obligation to provide access to remedies (Pillar 3). Under Pillar 2, businesses have the obligation to respect human rights and avoid contributing to harm through their operations. This involves conducting human rights due diligence (HRDD), which includes identifying, preventing, mitigating, and addressing risks related to their activities. Human rights impact assessments are a core component that requires companies to evaluate how their technologies might affect rights such as privacy, equality, and freedom of expression. Transparency is another cornerstone, requiring businesses to disclose how their technologies are developed and used, primarily when human rights implications exist. Furthermore, businesses must establish accessible grievance mechanisms to address complaints and provide remedies to individuals or communities harmed by their operations. Despite these responsibilities, challenges persist, including the non-binding nature of the UNGPs, competitive pressures that prioritise profit over ethics, and inconsistent industry standards. The case study, Tech Coalition's Lantern Program, designed to combat online child exploitation, provides an example of efforts to integrate UNGP principles through human rights due diligence and impact assessments. However, the voluntary nature of the UNGPs often limits their enforcement, leading to accountability gaps where competitive pressures in fast-evolving tech sectors may prioritise profit over ethical considerations.

Case Study: The Tech Coalition's Lantern Program

The Tech Coalition's Lantern Program, launched in 2023, is the first cross-platform signal-sharing initiative to combat online child sexual exploitation and abuse. This free program, now involving 21 tech companies like Meta, Google, Microsoft, and Snap, allows them to securely share "signals", anonymised intelligence about accounts, behaviours, or content violating child safety policies, using Meta's Threat Exchange platform. This helps platforms track and remove bad accounts while safeguarding privacy through privacy-by-design and eligibility checks. Before launch, the Tech Coalition commissioned a Human Rights Impact Assessment (HRIA) from Business for Social Responsibility (BSR) to identify risks, including the risk of erroneous account blocks. It engaged experts on child safety and digital rights for feedback. In its first transparency report (2023), Lantern showed participating companies acted on nearly 31,000 accounts, removed over 1,000 child sexual abuse material (CSAM) uploads, and deleted almost 400 related URLs. Recently, it's expanding to a pilot with financial institutions like Block Inc. to disrupt the money side of these crimes.

Regarding the other category of non-state actors, individuals or users of technologies, it is essential to refer back to Article 29 of the Universal Declaration of Human Rights. Article 29 states:

1. Everyone has duties to the community in which alone the free and full development of his personality is possible.
2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.
3. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

Nowadays, individuals have become vociferous users of emerging technologies such as AI apps and tools. For example, these technologies have given everyone the power not only to create messages in different formats (text, audio, visual or a combination of these) but also distribute them through social media platforms. While this enhances the right to freedom of speech and expression, if not used responsibly, it may harm others' enjoyment of rights, such as speech that dehumanises or stereotypes a particular community, or speech that is misogynistic. Article 29 of the UDHR underscores that humans live in a community with others, and it's only by living together that they can work towards the full development of their personalities. Thus, while exercising their rights and freedoms, they also have a duty towards others in the community - to respect the rights and freedoms of others and respect the just rules of morality, public order and general welfare in a democratic society. What are these just rules of morality, public order and general welfare in a democratic society? These rules may vary from society to society and will be reflected in a country's laws. However, some universal values are respect for human dignity, equality for all persons, equity, fairness, justice, and, above all, humanity.

Educational institutions play a crucial role in preparing individuals to navigate the complex relationship between technology and human rights. Universities and schools need to focus on digital skills to address human rights challenges arising from technological advancements. Their responsibilities extend beyond traditional teaching to integrating human rights into curricula, conducting research, and creating platforms for dialogue. For instance, universities may develop specialised courses that teach students to evaluate the impact of technology critically. Further, educational institutions - be it in the fields of health, environment, law, or others- can also play a role in the development of technologies that strengthen the enjoyment of rights.

Key Terms

- **Digital Literacy:** The ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies for employment, decent jobs, and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy.

- **Misogynist / sexist speech:** A form of hate speech that is gender oriented and specifically targets women.

1.2.3 Overview of Human Rights Mechanisms

At the international level, the United Nations has established specialised human rights mechanisms to monitor the implementation of human rights at the national level. These mechanisms include the Universal Periodic Review under the Human Rights Council, Constructive Dialogues held by expert bodies established under the core human rights treaties (also known as the treaty bodies) and Special Rapporteurs and Working Groups appointed by the Human Rights Council to monitor, investigate and report on specific human rights issues (thematic) or situations in particular countries (country - specific). These mechanisms are designed to respond, keeping human rights relevant amid rapid changes.

There are mechanisms at the regional level as well, such as the European Court of Human Rights, the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights, and the African Commission on Human and Peoples' Rights and the African Court on Human and Peoples' Rights. At the ASEAN level, there is the ASEAN-Intergovernmental Commission on Human Rights (AICHR). However, unlike other regional human rights mechanisms, AICHR cannot receive individual complaints or conduct independent investigations, and it focuses primarily on the promotion of human rights.

At the national level, the human rights mechanisms include courts and national human rights mechanisms. Apart from these formal mechanisms, civil society organisations acting as watchdogs, advocates, and enablers of community empowerment, international and regional organisations that bring in external expertise and experience, and media houses and journalists also play an important role in the promotion of human rights by raising awareness, highlighting harmful practices and calling for accountability.

You Are Here: Rights Matter When Things Go Wrong

Human rights rarely feel urgent when life is smooth. They matter most when something fails, when access is denied, when data is misused, or when a system treats you unfairly and you need protection, not explanations.

1.3 The Role of Technology in Promoting Human Rights

Technology has significant potential to promote human rights, justice, and empowerment.

1.3.1 Expanding access to information, education and healthcare

Technology has significantly enhanced access to information, education, and healthcare services. Innovations designed for the disability community often evolve to benefit society at large. For example, voice recognition systems such as Apple's Siri and Google Assistant were initially developed to assist individuals with limited dexterity or learning disabilities but are now widely used for convenience and productivity. Designing technologies with accessibility in mind not only promotes inclusion but also drives innovation, improves user experience, and stimulates economic growth. In healthcare, telemedicine bridges geographical barriers, while advanced diagnostic tools and treatments improve health outcomes. Likewise, digital technologies have broadened access to quality education, with AI-driven personalised learning systems helping students with diverse abilities achieve better learning results.

1.3.2 Strengthening human rights monitoring, accountability and legal empowerment

Advancements in data collection have transformed how human rights violations are documented and prosecuted. Satellites, drones, and smartphone footage enable tracking of combat zones and documenting transgressions as they occur. Advanced AI and machine learning can analyse large datasets to uncover systemic patterns of injustice, such as labour exploitation in supply chains. Digital platforms can also be created to provide legal education and access to legal aid and services, enabling legal empowerment of vulnerable populations.

1.3.3 Empowering marginalised communities and amplifying voices

Technology, and more specifically digital tools, have broken down traditional barriers, allowing minority groups to challenge repressive structures. Social media allows vulnerable groups, such as indigenous peoples and refugees, to create their own narratives, amplify their voices, and organise movements for change and justice. Blockchain technology provides pseudonymity, allowing activists to raise critical issues while protecting themselves from reprisals by the State. Further, affordable mobile and internet services have democratised the documentation and reporting of injustices, fostering a sense of global solidarity.

1.3.4 Facilitating democratic participation and civic engagement

Technology facilitates transparency in the political process, though it presents unique challenges. Blockchain technology, for example, promotes freedom of association by providing safe, collaborative platforms for civic activity. It also enables reliable online voting, allowing voters to cast encrypted ballots and ensure their votes are counted correctly. Digital tools enable people with disabilities to make educated decisions regarding political candidates. Blockchain also promotes participatory lawmaking by validating voter identities and facilitating support for community-driven legislative initiatives. While technology democratises communication by amplifying diverse viewpoints, social media algorithms frequently create "echo chambers" that reinforce pre-existing opinions, restricting exposure to new perspectives.

Reflection and Discussion:

Social media algorithms often create echo chambers. Should platforms in your country be legally forced to show users content from opposing views? Why or why not?

1.3.5 Supporting financial inclusion and economic empowerment

Digital innovation drives financial inclusion and economic empowerment. E-commerce platforms, mobile banking, and gig-economy apps create vital income opportunities and expand access to financial services for underserved populations. For example, in Indonesia, platforms like Gojek and Grab enable rural drivers and small vendors to join the gig economy, boosting livelihoods through accessible digital marketplaces. Similarly, mobile banking apps like GCash in the Philippines empower unbanked individuals to manage finances, pay bills, and access micro-loans, fostering economic independence.

1.3.6 Protecting cultural and environmental rights

Technology has substantially improved the protection of cultural and environmental rights in Southeast Asia, safeguarding history and encouraging sustainable environments. Digital archives, such as Cambodia's Bophana Audiovisual Resource Centre, digitise and preserve intangible cultural assets, including Khmer Rouge survivor testimonies and traditional performing arts, ensuring that languages and customs are preserved for future generations. Environmental monitoring technologies, such as drones and satellite imagery, are utilised in Indonesia to detect unlawful deforestation in Kalimantan's rainforests, increasing transparency and empowering communities to campaign for their right to a safe environment. Sensor networks in Vietnam monitor water quality in the Mekong Delta, helping local fishermen fight pollution. These advancements, when led by ethical principles and human rights frameworks, transform technology into a powerful instrument for cultural preservation, environmental justice, and inclusive empowerment.

1.4 The Adverse Impacts of Technology on Human Rights

While technology is positively transformative, it also enables new forms of harm. Far from neutral, its design and application reflect and shape societal values, making it a double-edged tool that can be exploited to undermine human rights if not guided by ethical principles and rigorous safeguards.

1.4.1 Eroding privacy

In the digital age, widespread surveillance poses a massive threat to privacy, weakening the enjoyment of human rights. The right to privacy, protected by Article 12 of the UDHR and Article 17 of the ICCPR, is one of the rights most heavily affected by modern technology. We examine the legal foundations and significant threats in Chapter 2.

Governments and companies use the same digital infrastructure that enables communication, such as smartphones, social media, and internet services, to monitor online activity, track physical movements via GPS, and collect massive amounts of personal data. This approach, known as "surveillance capitalism," entails gathering and analysing user data to predict and influence behaviour, frequently without transparency or accountability. Biometric technologies, such as facial recognition and fingerprint scanning, exacerbate these issues due to their intrusive nature and the irreplaceability of compromised biometric data. Large-scale databases are still vulnerable to hackers, exposing individuals to identity theft and unauthorised profiling. The advent of "digital authoritarianism" sees governments using tools like social media monitoring and spyware to repress dissent and control public discourse, generating a terrifying "Panopticon" environment that undermines free expression and trust in institutions. Even well-intentioned initiatives, such as AI-powered systems to combat human trafficking, might violate privacy by intercepting encrypted communications.

Reflection and Discussion:

- *In an era when mass data collecting is both practical and cost-effective, does using a smartphone or social media imply a voluntary loss of privacy rights under UDHR Article 12?*
- *When does the ease of digital technologies turn into a forceful surrender of personal information?*

1.4.2 Amplifying Discrimination and Exacerbating Inequality

Technology frequently reinforces power inequalities and exacerbates inequality rather than reducing it, benefiting the privileged while marginalising vulnerable people. Algorithms for hiring, credit scoring, and predictive policing that are trained on biased historical data might perpetuate social preconceptions, resulting in unfair outcomes for marginalised communities seeking employment, financial services, or justice. For instance, AI models trained primarily on Western-centric data can overlook or inaccurately represent people in Southeast Asia, given the region's linguistic, skin-tone, and cultural diversity. AI in credit scoring can disproportionately penalise low-income individuals or marginalised groups, leading to unfair loan denials or higher interest rates. These approaches have the potential to reinforce systemic disparities rather than promote fairness. The digital gap worsens this problem, as access to technology remains unequal due to differences in income, geography, gender, age, and education. Digital improvements often focus on urbanised economies, leaving rural and underdeveloped regions behind, thereby widening socioeconomic divides. Technology transfer from the Global North frequently maintains these imbalances, resulting in disparities in design and deployment. For example, the transition to automated teller machines (ATMs) that are not built for visually impaired users in banking systems denies these people financial access. If market-driven innovation inevitably favours the wealthy, can technologies produced by for-profit entities actually maintain equality and non-discrimination?

FinTech companies are increasingly using AI algorithms to enhance predictive accuracy and streamline loan approvals, analysing a broader range of traditional and non-traditional data, including social media activity and online purchasing behaviour. While this can expand access to credit, particularly for those with limited traditional credit history, it also raises substantial human rights concerns, especially regarding discrimination against low-income individuals and marginalised communities. For example, when AI-driven lending algorithms were used, concerns were raised about a lack of transparency, as borrowers were not informed of the criteria used for creditworthiness assessments or the reasons for loan denials.

1.4.3 State Control, Censorship, and Restrictions on Freedoms

The control of information through censorship and content regulation endangers freedom of expression (ICCPR Article 19) and the right to information. Advanced technologies enable governments to control communication networks by employing measures such as internet shutdowns, filtering systems, and ambiguous cybersecurity laws to repress dissent and rule civic areas. Some regimes have used internet blackouts to quell opposition. At the same time, broad-based legislation allows authorities to monitor platforms, erase content labelled as "false," and criminalise criticism, frequently targeting bloggers and activists. Digital surveillance, which is commonly undertaken with little oversight, tracks activists and creates an environment of fear, deterring civic involvement and undermining civil society and democratic processes. Furthermore, powerful online gatekeepers, such as Facebook and Google, regulate content in ways that limit free speech, removing posts for alleged copyright violations or graphic content without adhering to human rights standards. While cybersecurity laws seek to address serious threats such as cyber-fraud and terrorism, they often grant governments broad authority to restrict fundamental liberties in the name of cybersecurity and national security.

Reflection and Discussion:

Vietnam's 2024 Cybersecurity Law lets the government remove "false" posts within 24 hours. Is this a reasonable way to fight disinformation, or does it give the state too much censorship power?

1.4.4 Spreading Misinformation, Disinformation and Polarising Society

While digital platforms are great communication tools, they are also very susceptible to manipulation, amplifying disinformation and creating divided cultures. The anonymity and broad reach of these platforms enable the rapid dissemination of disinformation (erroneous information) and hate speech, which is often further exacerbated by algorithms that prioritise sensational material to drive user engagement. For example, internet disinformation campaigns have fuelled violence and discrimination against minority groups, demonstrating the real-world consequences of these digital dynamics. Algorithmic content curation generates filter bubbles and echo chambers, reinforcing pre-existing opinions, limiting exposure to alternative perspectives, and generating conditions conducive to the spread of disinformation. Furthermore, technology enables online abuse, which disproportionately affects vulnerable groups such as women and LGBTQ+ individuals, thereby silencing their views and risking personal safety. Computational propaganda, fuelled by organised cyber troops, further influences public perception, widening socioeconomic gaps.

Because of the proliferation of user-generated content on social media platforms, corporations are increasingly turning to AI-driven content moderation to tackle harmful content such as misinformation and hate speech. However, this poses a significant challenge to freedom of expression, especially in linguistically and culturally diverse contexts such as Southeast Asia. AI technologies, including Natural Language Processing (NLP) and Natural Language Understanding (NLU), analyse text to identify harmful language patterns, but often struggle with contextual nuances, sarcasm, and local idioms. For instance, racial and religious hate speech online is a growing concern. Still, AI systems may fail to accurately detect offence because they cannot understand local context, where certain words that are innocuous in one setting can be highly offensive in another. AI moderation tools are primarily trained on Western-language datasets, which may either over-censor legitimate expression or under-enforce local regulations, leading to accusations of censorship and inconsistency. The ability of algorithms to amplify sensational and emotionally charged content also contributes to the polarisation of communities.

1.4.5 Challenges to Accountability, Justice, Ethics and Human Agency

Emerging technologies call into question accountability, justice, ethics, and human agency, reshaping the mechanisms that protect human rights. Accountability challenges stem from the "black-box" nature of many advanced AI models, where their decision-making processes are not easily interpretable. This opacity makes it difficult to determine who is responsible when an AI system causes harm or makes biased decisions, complicating legal redress for affected individuals. Automated systems distort accountability by making

judgments appear unavoidable rather than human-driven. For example, in some areas, prepaid water meters automatically turn off supplies to low-income residents, concealing human rights violations behind technological procedures. Similarly, autonomous weapons such as drones and military robots divide culpability in conflict, making it difficult to assign blame for violations of international humanitarian law, whether to the programmer, manufacturer, commander, or operator.

Misuse of sensitive data in the health sector, such as AI-driven profiling, can lead to discrimination, such as insurance denial based on biased algorithms. The economic consequences are as severe: automation and AI replace low-skilled occupations, causing unemployment and insecurity, while gig economy platforms frequently abuse workers through unstable contracts, poor wages, and the absence of safeguards such as healthcare. Advanced biomedical technologies, while beneficial, pose ethical challenges, such as the genetic editing of embryos to achieve desired traits. In Southeast Asia, these dynamics are reflected in the fast use of AI and automation, which magnifies both benefits and hazards. These difficulties emphasise technology's dual nature: as a tool for empowerment and rights expansion, it can also be a source of injustice, harm, and decreased freedoms.

In short, technology, much like any tool, can be utilised for both positive and negative purposes. Its impact on human rights varied, presenting a complex landscape of opportunities and challenges. Table 1.2 provides a clear understanding of the dual-edged impact of technology across different areas of human rights.

Table 1.2: Positive and Negative Impacts of Technology on Human Rights

Area of Human Rights	Positive Impacts of Technology	Negative Impacts of Technology
Freedom of Expression	- Social media platforms enable greater expression and activism. - Real-time reporting of human rights abuses amplifies marginalized voices.	- Governments use digital surveillance to monitor and censor dissenting voices. - Algorithms promote disinformation and hate speech, polarizing societies.
Privacy	- Encryption tools (e.g., WhatsApp) allow secure communication. - Privacy regulations promote responsible data use.	- Mass data collection and surveillance technologies erode privacy rights. - Biometric databases are often hacked or misused, leading to identity theft.
Access to Justice	- Digital platforms provide legal aid and resources to marginalized groups. - AI systems help identify patterns of injustice and human rights violations.	- Limited digital literacy prevents equitable access to legal tools. - Use of biased AI algorithms can lead to unfair judicial outcomes.
Right to Information	- Open data initiatives provide greater transparency (e.g., budget spending and election results). - E-learning tools empower individuals with knowledge about their rights.	- Internet shutdowns and content filtering restrict access to information. - Manipulation of search engine results can mislead public understanding of rights issues.
Freedom of Assembly and Association	- Online platforms facilitate organization of protests and human rights campaigns. - Crowdfunding platforms support civil society initiatives.	- Digital surveillance discourages participation in activism due to fear of reprisals. - Cyberattacks on activists and NGOs disrupt operations and create fear.
Equality and Non-Discrimination	- AI tools identify discriminatory practices and help craft inclusive policies.	- Algorithmic biases perpetuate racial, gender, and socioeconomic discrimination.

Area of Human Rights	Positive Impacts of Technology	Negative Impacts of Technology
	- Social media campaigns promote inclusivity and awareness of minority rights.	- Online harassment disproportionately targets vulnerable groups, silencing them.
Right to Work	- Platforms like LinkedIn provide job opportunities and professional networking. - E-commerce platforms empower entrepreneurs to access broader markets.	- Automation and AI threaten traditional employment sectors, particularly for low-skill workers. - Gig economy platforms often exploit workers through unfair contracts and lack of benefits.
Health and Well-being	- Telemedicine expands access to healthcare for rural communities. - AI supports faster diagnoses and personalized treatments.	- Health data breaches compromise patient confidentiality. - Misuse of health data for discriminatory purposes (e.g., denying insurance).
Education	- Digital tools and Open Educational Resources (OER) expand access to quality education. - AI personalized learning enhances outcomes for students with diverse needs.	- Unequal access to technology widens the education gap between urban and rural areas. - Over-reliance on EdTech risks commodifying education, undermining its holistic value.
Freedom from Torture and Inhuman Treatment	- Technology exposes abuses and provides evidence for prosecution (e.g., use of smartphones to document crimes). - Drones and satellites monitor conflict zones, aiding humanitarian efforts.	- Torture-enabling technologies (e.g., spyware) facilitate tracking and abuse of dissidents. - Dual-use technologies are exploited for oppression under authoritarian regimes.
Cultural Rights	- Digital archives preserve and promote Southeast Asian cultural heritage.	- Globalization of content threatens local cultures and languages through digital homogenization.
Environmental Rights	- Technology enables environmental monitoring, promoting accountability for human rights violations related to climate change.	- Industrial use of technology contributes to environmental degradation, affecting livelihoods and health.

Reflection and Discussion

Facial recognition technology is widely used for security, law enforcement, and commercial purposes, but it raises serious concerns about privacy, consent, and the potential misuse or compromise of biometric data. Reflect on the implications of having your facial data stored in a database:

- How does this impact your privacy and autonomy?
- What specific regulations should governments implement to ensure authorities use facial recognition responsibly?
- Should its use be paused or banned until robust safeguards are established, or can its benefits, such as enhanced public safety, justify its application if strictly regulated?
- Discuss how to balance the technology's advantages against the risks it poses to individual rights and societal trust.

You Are Here: You Will Be Asked to Trust Invisible Systems

Many decisions affecting your future will be made quietly by systems you never see. Learning about rights gives you a way to question that silence, and to decide when trust should be earned, not assumed.

1.5 Conclusion

Technology is never just technology; it is always a mirror of the values we choose to embed in it. The same smartphone that lets a student in a remote Philippine province attend online classes can also track her location without consent. The same AI that helps doctors in Jakarta diagnose diseases faster can quietly discriminate when hiring the next generation of workers. This double-edged reality is the heart of everything we will study together. What we have seen in this chapter is that human rights do not stop at the edge of the digital world; they must travel with us into every app, platform, and device. When technology is designed and governed with care, it becomes a powerful ally for freedom, equality, and dignity. When it is not, it can deepen division, silence voices, and erode trust. The good news is that the future is not already written. Students, activists, developers, policymakers, and ordinary users like you have the chance to demand and create technology that serves people rather than exploits them.

Key Takeaways

1. Modern technologies (AI, IoT, big data, blockchain, etc.) are interconnected and changing society faster than ever before.
2. Every category of human rights, civil, political, economic, social, cultural, environmental, and digital, is directly affected by digital tools.
3. Technology can expand access to education, healthcare, and justice, and amplify marginalised voices, but only when designed inclusively.
4. The biggest risks today include mass surveillance, algorithmic discrimination, censorship, misinformation, and the widening digital divide.
5. Companies, governments, and citizens all share responsibility for making technology respect human rights.

Issues to Think About

1. Which app or device do you use every day that feels empowering, and which part of it worries you the most about your rights?
2. If internet access disappeared from your campus tomorrow, which of your rights would be affected first, and why?
3. Think of a recent news story from your country involving technology (data leak, deepfake, internet shutdown, etc.). Which human right was most clearly at stake?
4. When you post on social media, do you feel completely free to speak, or do you sometimes hold back? What makes the difference?
5. Imagine you could add one new rule to every tech company operating in your country. What would it be, and which right would it protect?
6. Ten years from now, what kind of digital society do you want to live in, and what can you start doing today to help make it happen?

Further Readings

Office of the United Nations High Commissioner for Human Rights. (2025). *The right to privacy in the digital age: Focus on discrimination and unequal enjoyment of the right to privacy in the context of data collection and data processing*. (A/HRC/60/45). United Nations. https://www.ohchr.org/en/privacy-in-the-digital-age/reports

Office of the United Nations High Commissioner for Human Rights. (2025). *Human rights due diligence for digital technology use*. United Nations. https://www.ohchr.org/sites/default/files/2025-09/ohchr-brief-ai.pdf

Amnesty International. (2025). *The state of the world's human rights: April 2025*. https://www.amnesty.org/en/documents/pol10/8515/2025/en/

Human Rights Watch. (2025). *World report 2025*. https://www.hrw.org/world-report/2025

Freedom Online Coalition. (2025). *Joint statement on artificial intelligence and human rights*. https://freedomonlinecoalition.com/joint-statement-on-ai-and-human-rights-2025/

United Nations. (2025). *Governing AI for humanity: Final report*. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

United Nations Conference on Trade and Development. (2025). *Technology and innovation report 2025: Inclusive artificial intelligence for development*. https://unctad.org/system/files/official-document/tir2025_en.pdf

Wagner, B., Kettemann, M. C., & Vieth-Ditlmann, K. (Eds.). (2025). *Research handbook on human rights and digital technology* (Updated ed.). Edward Elgar Publishing. https://www.elgaronline.com/edcollbook/book/9781035308514/9781035308514.xml

Alegre, S. (2024). *Human rights, robot wrongs: Being human in the age of AI*. Atlantic Books. (Accessible via publisher previews and libraries; ISBN: 9781838951931)

UNESCO. (2025). *Report of the Independent Expert Group on Artificial Intelligence and Culture*. https://articles.unesco.org/sites/default/files/medias/fichiers/2025/11/CULTAI_Report%20of%20the%20Independent%20Expert%20Group%20on%20Artificial%20Intelligence%20and%20Culture%20%28final%20online%20version%29%201%20%281%29.pdf

Chapter 2:

Legal and Policy Frameworks: Human Rights in the Digital Realm

Reader's Guide

Welcome to the chapter that answers the big question: Who is actually responsible when technology harms human rights? Is it the government, the tech company, the app developer, or all of us? Here, you will discover the existing standards (international treaties, ASEAN declarations, national laws) and the gaps that still leave people vulnerable. Using real examples, we will see how the world is slowly catching up with fast-moving technology. By the end, you will be able to judge whether today's laws and promises are strong enough for our digital reality, or whether we still need much stricter rules. In this chapter, you will:

- Learn the key UN human rights standards pertaining to the digital realm.
- Explore ASEAN's frameworks, their strengths, and their limits.
- Discover why accountability is still so hard and what solutions are emerging around the world.

Key Terms

- **Due Diligence**: the process through which companies identify, prevent, mitigate, and account for how they address actual or potential human rights impacts. It ensures that organisations act responsibly and do not contribute to harm.
- **Remedy**: the actions or measures taken to address, correct, or compensate for harm or rights violations. It ensures that individuals can seek justice and have the harm acknowledged and repaired.
- **Non-Retrogression**: means that governments must not roll back or diminish the level of economic, social, and cultural rights already enjoyed by people, unless there are exceptional and fully justified circumstances.
- **Soft Law :** non-binding rules, principles, guidelines, or standards that influence behaviour but do not have legal enforceability. Examples include declarations, codes of conduct, and voluntary frameworks. Although not legally binding, soft law can shape norms, guide state or corporate behaviour, and pave the way for future binding regulations.
- **Hard Law**: legally binding rules found in treaties, legislation, and regulations that create clear legal obligations for states or other actors. Hard law can be enforced through courts or formal legal mechanisms, and violations may lead to penalties or legal consequences.

2.1 International Legal Framework

Article 12 of the Universal Declaration of Human Rights (UDHR) which recognises the right to privacy. It guarantees that no one should be subjected to arbitrary interference with their privacy and protects them from such interference or attacks. The right is reaffirmed in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). At the time, the UDHR and ICCPR were drafted, the understanding of privacy and correspondence was different. There were no digital technologies such as smart gadgets, communication media such as email and chat applications, or CCTVs (closed-circuit televisions) that could collect information about our private lives. Thus, these rights need to be interpreted in sync with the present times. The UN Human Rights Council Resolutions 68/167 (2014) and A/HRC/34/L.7 (2017), together with the 1990 UN Guidelines on Computerised Personal Data Files, have recognised that privacy rights as recognised in the UDHR and ICCPR apply online. They have recognised that mass surveillance and unchecked data collection are illegal unless they are strictly lawful, necessary, proportionate, and supervised by judges, and people should not be targeted just for their opinions. Companies must actively respect these rights through due diligence and remedies; encryption and anonymity tools must be protected, not weakened; and vulnerable groups (journalists, children, activists) must be provided with extra safeguards. (See Table 2.1)

Collectively, these international instruments and frameworks form a comprehensive system that safeguards individual rights while enabling states to address legitimate security concerns through technological means.

Reflection and Discussion:

- *Is your smartphone like your "home"?*
- *Is your browsing history your correspondence?*
- *When you send a picture to a friend on Instagram, is this private or public communication?*

You Are Here: Why Law Feels "Late"

Many technology harms are addressed only after damage has already occurred, after a data leak, a biased decision, or a surveillance scandal. This is why legal frameworks often feel slow or reactive. Understanding law helps you see both its limits and why prevention matters.

Table 2.1: UN Standards on Human Rights in the Digital Realm

Article	Full Text / Key Excerpt	Core Meaning for Tech
Article 12, UDHR	"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."	Protects personal life from snooping (e.g., data collection, surveillance)
Article 17, ICCPR	"1. 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. 2. Everyone has the right to the protection of the law against such interference or attacks."	Stronger version of UDHR 12: requires laws prohibiting digital surveillance without oversight; calls for judicial review and business accountability

Article	Full Text / Key Excerpt	Core Meaning for Tech
UN HRC Resolution 68/167 (2014) & A/ HRC/34/L.7 (2017)	Reaffirms UDHR 12/ICCPR 17 apply online; condemns unlawful surveillance/data collection; urges judicial oversight, proportionality, business accountability; protects encryption/anonymity	Privacy rights are the same offline and online; states/companies must respect them. Emphasises vulnerable groups (journalists, children); calls for transparent data practices and cross-border cooperation
UN Guidelines for Regulation of Computerized Personal Data Files (1990)	Principles: consent, purpose limitation, security, transparency, access/correction rights, accountability, data minimization	Framework for data protection laws; data must be collected fairly and used only for stated purposes. nfluences national laws; non-binding but widely adopted (e.g., in ASEAN Data Protection Framework)
Charter of Human Rights and Principles for the Internet	Outlines 10 core principles for the internet, covering universality, accessibility, neutrality, rights, expression, privacy, diversity, governance, standards and regulation as well as life liberty and security.	Serves as a global rights-based framework for protecting human dignity, equality, and justice online.
APC Internet Rights Charter	Groups 31 rights into 7 themes: access, freedom of expression, privacy, governance, participation, diversity, and gender equality.	Advocates for inclusive, democratic, and equitable Internet access across regions, emphasizing empowerment and accountability.
UNESCO Internet Universality Indicators (R.O.A.M. Framework)	Promotes an Internet that is Rights-based, Open, Accessible, and Multi-stakeholder participation (R.O.A.M.).	Encourages governments to develop policies rooted in human rights and to monitor digital inclusivity and openness.
UNESCO Recommendation on the Ethics of Artificial Intelligence	Establishes global ethical standards for AI emphasizing human rights, fairness, transparency, privacy, accountability, and sustainability.	The first global normative framework for AI ethics; calls for institutional oversight and human rights–based AI governance.

2.2 Regional Legal and Policy Frameworks

The Association of Southeast Asian Nations (ASEAN) plays a central role in shaping how technology intersects with human rights. ASEAN, founded in 1967, includes 10 member countries and aims to promote economic growth, peace, and stability. However, when it comes to technology and human rights, progress has been slow and uneven. ASEAN's core principles, such as non-interference in each other's internal affairs and decision-making by consensus, make it difficult to create strong, unified rules that everyone must follow. This means that while some countries advance quickly in digital innovation, others still lag behind, creating gaps in protecting rights like privacy and free speech.

At the heart of ASEAN's human rights efforts is the **ASEAN Human Rights Declaration (AHRD) 2012.** This instrument recognises the rights of people, including the right to privacy, freedom of expression, and access to information. However, the AHRD lacks enforceability. The result is that human rights standards are best protected through international treaties and not the ASEAN Declaration. This is true not only for the AHRD, but also for many of the standards discussed below. The ASEAN Intergovernmental Commission on Human Rights (AICHR), while providing a platform for discussion, also lacks protection powers, limiting its ability to address rights violations effectively.

Table 2.2 presents key ASEAN instruments that have the potential to address the intersections between technology and human rights.

Table 2.2: ASEAN Human Rights & Technology Dashboard 2025

ASEAN Instrument (year)	Main topic	Key promise
ASEAN Human Rights Declaration (AHRD) 2012	All rights	Privacy + free expression for everyone
ASEAN Framework on Personal Data Protection 2016	Data privacy	Consent, security, transparency
ASEAN Master Plan on Connectivity 2025	Connectivity and Infrastructure	Build physical/digital links for inclusive growth (5G, e-gov, sustainable urban corridors)
ASEAN Guide on AI Governance and Ethics 2024	Artificial Intelligence	Transparency, fairness, fairness, human oversight
ASEAN Responsible AI Roadmap (2025-2030)	Responsible AI Implementation	Step-by-step actions for ethical AI
ASEAN Cybersecurity Cooperation statements 2018–2024	Surveillance & cyber laws	Fight cybercrime together

The ASEAN Framework on Personal Data Protection, adopted in 2016, is a non-binding regional guideline. It aims to harmonise data protection standards across ASEAN member states to foster trust in the digital economy, facilitate cross-border data flows, and support e-commerce growth, while respecting individual privacy rights. It draws from global principles like the OECD Privacy Guidelines and APEC Privacy Framework, emphasising on certain core elements: consent and purpose specification (data collection must be informed and limited); accuracy and security of data; transparency through privacy notices; access and correction rights for individuals; accountability of organisations via policies and audits; minimisation and retention limits; and cross-border transfer safeguards (e.g., adequate protection in recipient countries). It is not enforceable, and there is no accountability mechanism attached to it.

Closely linked is the **ASEAN Master Plan on Connectivity 2025** (MPAC 2025), which is a major regional strategy designed to achieve a seamlessly connected and integrated ASEAN that promotes competitiveness, inclusiveness, and a heightened sense of Community. MPAC 2025 outlines five strategic priorities: sustainable infrastructure, digital innovation, seamless logistics, regulatory excellence, and people mobility. Significantly, the framework integrates environmental concerns, highlighting the importance of "environmentally sustainable land transport corridors" and promoting smart urbanisation under its sustainable infrastructure focus. Initiatives like the **ASEAN Sustainable Urbanisation Strategy (ASUS)** stem directly from the MPAC 2025. This recognises that good connectivity supports rights like education (through online learning) and health (via telemedicine apps). However, implementation varies: wealthier urban areas might get fast internet quickly, while remote villages face delays, widening inequalities and affecting social rights.

In line with the ASEAN Community Vision 2025, ASEAN member states adopted the **ASEAN Digital Masterplan (ADM) 2025**. It is a strategic five-year roadmap (2021–2025) to transform the region into a leading digital community and economic bloc powered by secure, innovative digital services, technologies, and ecosystems Eight key outcomes are listed: improved fixed and mobile broadband infrastructure, trusted digital services with consumer harm prevention, competitive digital supply markets, expanded e-government usage, business connectivity for cross-border trade, increased digital participation for businesses and individuals, and digital inclusion to bridge urban-rural and socioeconomic divides. Through regulatory harmonisation, talent development (e.g., coding skills and hackathons), sustainable investments in connectivity and cloud services, and multi-stakeholder collaboration involving governments, it aims to close digital gaps and overcome implementation hurdles. This plan simply helps to drive economic growth, for example, helping small businesses sell products online, while ensuring no one is excluded.

The ASEAN Guide on AI Governance and Ethics, released in 2024, encourages ethical use of AI. It promotes best practices like fairness (avoiding bias in AI decisions) and transparency (explaining how AI works). By comparison, the European Union's AI Act classifies AI systems used in employment, such as recruitment tools, worker-monitoring software, and performance-evaluation algorithms, as "high-risk". The EU AI Act requires providers and deployers to conduct fundamental rights impact assessments, ensure human oversight, maintain transparency about automated decision-making, and implement bias-mitigation measures. In contrast, ASEAN's guide is voluntary and flexible.

The **ASEAN Responsible AI Roadmap (2025–2030)**, adopted on March 5, 2025, serves as a practical, actionable strategy to help ASEAN member states (AMS) develop and deploy responsible AI in ways that are inclusive, sustainable, and tailored to the region's diverse needs and capabilities. It complements the earlier ASEAN Guide on AI Governance and Ethics (2024) and its 2025 expansion on generative AI by moving from principles to step-by-step implementation. The Roadmap focuses on two main areas:

- Foundational elements: Policy, regulation, infrastructure, and capacity-building to create an enabling environment for responsible AI.
- Targeted actions: Specific initiatives like enhancing public-sector AI use, building regional partnerships, securing data-sharing platforms, inclusive community engagement, and multi-stakeholder governance.

Key priorities include skills & capacity building, fairness & inclusion, governance & participation, and regional integration & cooperation. It introduces a Readiness Assessment Framework (categorising countries into levels) and is supported by the ASEAN AI Safety Network (AI SAFE), established in October 2025 as the world's first regionally endorsed AI safety body. Like most ASEAN tech documents, it is non-binding and consensus-driven, emphasising interoperability with global standards while respecting national differences. By 2030, it aims to make Southeast Asia a leader in ethical, human-centered AI that drives economic growth without leaving anyone behind.

The ASEAN statements and plans on cybersecurity cooperation (2018–2024) further aim to strengthen joint responses to cybercrime, improve information-sharing, and build technical capacity across the region. While their primary focus is on issues such as ransomware, data breaches, and cross-border online fraud, these documents have also been referenced by several member states in the drafting of national cybersecurity laws. These national laws often include provisions on data localisation, rapid content removal, and government access to user data, measures intended to enhance security but which, in practice, can affect the rights to privacy and freedom of expression. Because the ASEAN framework itself is non-binding and contains no explicit human-rights safeguards, its implementation at the national level has varied widely: some countries have used it to justify broader state oversight of online platforms, while others have emphasised technical cooperation. As a result, the same initiative that helps combat genuine cyber threats has also become linked to laws that, in certain contexts, restrict digital rights.

ASEAN is further expanding its efforts through initiatives such as the **ASEAN Digital Economy Framework Agreement** (DEFA), initiated in 2023, with signing targeted for 2026. This agreement aims to create unified rules for digital trade, potentially becoming the world's first region-wide digital economy pact, boosting jobs and innovation. Negotiators have inserted provisions on data protection standards, digital inclusion, and SME participation. However, because the text remains consensus-driven and contains carve-outs for "national security" and "public morals," critics worry that strong economies will benefit most, while weaker enforcement in other member states could leave privacy, labour rights, and marginalised communities unprotected.

The ASEAN Smart Cities Network (ASCN), launched in 2018, uses technology to support sustainable cities, such as smart traffic lights that reduce pollution, but challenges remain, especially for marginalised groups, like low-income residents who might not benefit from high-tech solutions. ASEAN also upgraded its ASEAN Telecommunications and IT Ministers Meeting (TELMIN) to the ASEAN Digital Ministers Meeting (ADGMIN) in 2021, broadening discussions to include cybersecurity, innovation, and free speech.

Despite these frameworks, ASEAN continues to face ongoing issues. The non-interference principle often prevents collaborative action against digital rights violations, like censorship or unequal tech access. Weak enforcement, varying country capacities, and fragmented rules mean human rights protections differ widely, stronger in some places, weaker in others.

Case Study: ASEAN's Technological Response to Human Trafficking and Online Scam Factories

Human trafficking in Southeast Asia violates numerous human rights. People's lives are threatened, their labour is exploited, and they can even be charged with a crime because they have had their identification and travel documents stolen. Traffickers increasingly leverage digital platforms for recruitment through fraudulent job advertisements, exploiting victims for forced labour and sexual slavery. ASEAN and its member states have responded with policies and technological measures, yet trafficking has not stopped.

The ASEAN Convention Against Trafficking in Persons, Especially Women and Children (ACTIP) is central to regional efforts, emphasising victim protection, prosecution, and prevention aligned with human rights principles. ASEAN initiatives, such as digital monitoring systems and joint rescue operations, have successfully dismantled trafficking networks. Awareness campaigns further reduce vulnerabilities by educating at-risk communities, often funded by ASEAN and member states. While these are important activities, they may not help people trafficked from outside the region, nor can they help people who lose all their life savings to online scams run from scam centres which rely on trafficked labour.

The technology responses of member states to combat trafficking can both protect people's rights and violate them. For example, Thailand uses AI-powered tools to monitor encrypted communications and online trafficking operations. While this may save some people from being trafficked, it also raises concerns about privacy violations. Similarly, the unequal distribution of technological resources also exacerbates rights inequalities. Singapore has the technology to effectively deploy AI for tracking trafficking activities. It can also intervene to prevent falling for scams by increasing awareness of online transactions. Nations like Laos and Myanmar lack the infrastructure to replicate such measures, affecting the equitable protection of victims across the region.

There are many stakeholders in responding to human trafficking in the scam factories.

ASEAN has a duty to ensure that legal standards protecting human rights are harmonised across the region.

Technology companies, such as Facebook, TikTok, and Telegram, should monitor online activity to ensure people are not deceived into a trafficking situation or scammed.

Banks should have protections in place so people do not lose their money to scams

ASEAN and States should ensure the technology to confront trafficking is equitably spread across ASEAN countries by addressing the digital divide among member states

People using social media should be educated about scams and false claims that could lead to trafficking, and they should report such messages to authorities.

This case illustrates how regional collaboration and technology can address trafficking but underscores the need for stronger human rights safeguards.

Reflection and Discussion:

- Should there be limits on the extent to which governments may snoop on online activities to arrest traffickers? What kind of personal info should stay private, and why?
- How can ASEAN help countries like Laos and Myanmar get the same anti-trafficking tech as Singapore? What is one creative idea to close this gap?
- What can platforms like TikTok or Facebook do to stop traffickers' fake job ads? How can students help spot and report these scams?
- Imagine you are on a student council advising ASEAN. What is one fun, practical way to teach your peers about avoiding online scams and trafficking traps?

2.3 National Legal Frameworks

Southeast Asian nations have incorporated international human rights standards into domestic policies through legislation, institutional arrangements, and policy initiatives. They recognise the UDHR, signalling a commitment to uphold rights such as privacy, free speech, and assembly. However, these commitments are often undermined by national laws, weak enforcement mechanisms, limited resources, and a lack of political will. This gap between legal frameworks and their practical application diminishes the effectiveness of human rights protections, particularly in the context of technology.

A critical issue in the region is the lack of transparency and accountability in the development and implementation of technology-related laws. Policies governing surveillance technologies and online content regulation are often not rights-based, meaning their objectives are not to protect people's rights but to empower the government, increasing the risk of abuse and human rights violations. For example, stringent content regulation in some countries has been criticised for restricting freedom of expression under the guise of national security or public order.

Some ASEAN countries have proactively adopted strategies for emerging technologies such as AI. Singapore and Malaysia, for instance, have developed AI frameworks emphasising ethical governance, economic growth, and skills development. It is important to note that the government highlights the ethical use of AI, not a rights-based use. While ethical use definitely has its advantages, it does not protect people as vigorously as human rights. Conversely, several ASEAN States lack formal AI policies, reflecting uneven digital readiness and strategic planning, which complicates regional cooperation and leaves them vulnerable to unregulated AI applications and associated human rights risks.

National courts play a vital role in interpreting international human rights norms within domestic contexts. If national laws align with global standards, courts can contribute to rights-based frameworks that uphold freedoms while balancing concerns such as national security. However, in most cases, restrictive laws on public order and online freedom of expression enable States to quash their critics and threaten their opponents. At this point in history, various soft law instruments and industry-led initiatives have emerged to address the ethical and human rights implications of technology. Still, they have not been harmonised across the region, and they struggle to keep up with rapid technological innovation. A few critical areas, particularly on data protection, cybersecurity and AI regulation, are further discussed below.

You Are Here: No Rules Also Means No Protection

When technology operates without clear rules, people are left to deal with problems on their own. Inaction can quietly favour those with power, while everyone else absorbs the risks.

2.3.1. Data Protection Laws in Southeast Asia

Personal Data Protection (PDP) concerns the safeguarding of any information related to an identified or identifiable natural (living) person, including names, biometric data, IP addresses, and communication content. It is instrumental in enabling other rights and freedoms, such as free speech and the right to assembly, particularly in the digital age. Key aspects of data protection include:

- Security: This involves protecting personal data from unauthorised access, loss, or destruction, using technologies and measures such as firewalls, encryption, and intrusion detection systems. AI systems should also protect confidential information in line with international standards and establish safeguards against cyber threats.
- Fair and Legitimate Processing for Specific Purposes with Consent: Data must be processed lawfully, fairly, and transparently, and collected only for specified, legitimate purposes. Informed consent is a critical principle that emphasises that individuals must agree to the collection and use of their data, fully understanding how it will be collected and processed. This is crucial for maintaining user trust and complying with data protection regulations.
- Purpose Limitation: Personal data collected for specified, explicit, and legitimate purposes should not be further processed in a manner incompatible with those purposes.

- Data Minimisation: This principle dictates that only data necessary for the specified, legitimate purposes should be collected, thereby reducing the risks associated with excessive data collection.
- Storage Limitation: Data should not be kept longer than necessary for the purposes for which it was collected.
- Data Subject Rights: Individuals have rights over their personal data, including the right to access their data, the right to rectification (correction), and the right to object to its processing.
- Right to Erasure ("Right to be forgotten"): This allows individuals, under certain conditions, to request that search engines remove links to personal information when such information becomes excessive or irrelevant. This right necessitates a balance between individual privacy and economic interests or public access to information.
- Secured Cross-Border Data Transfer: Data protection also encompasses policies and mechanisms for secure cross-border data transfers.

Data protection laws in Southeast Asia illustrate the region's fragmented approach. Most ASEAN countries have adopted national data protection laws or have equivalent standards in their civil laws. Those without PDP laws are developing new laws in this area to protect people's personal information. Singapore and Malaysia lead with frameworks such as the Personal Data Protection Act (PDPA), which ensure privacy safeguards in a data-driven world. At the same time, some countries are still developing comparable regulations, creating inconsistencies that hinder cross-border data governance and expose privacy vulnerabilities (See Table 2.3).

Table 2.3: Data Protection laws in ASEAN countries (as of October 2025)

Country	Key Law(s)	Key Features & Exceptions
Brunei	Personal Data Protection Order (PDPO)	Consent-based processing, rights to access/correction; applies to private/public sectors; exceptions for national security, law enforcement.
Cambodia	Draft Law on Personal Data Protection (LPDP)	Proposed consent, security, and cross-border rules; extraterritorial; exemptions for security; interim telecom sector rules only.
Indonesia	Personal Data Protection Law (PDP Law)	Breach notifications (72hr), impact assessments; extraterritorial; government surveillance exceptions; fines up to 2% revenue.
Laos	Law on Protection of Electronic Data	Covers electronic data consent, accuracy, retention; limited scope/no dedicated authority; security exemptions; uneven enforcement.
Malaysia	Personal Data Protection Act (PDPA)	Private sector focus: consent, security, access rights; excludes government; 2024 adds breach notifications (72hr); fines up to RM 1M.
Myanmar	Protecting the Privacy and Security of Citizens Law	Basic protections against unauthorized interception; citizen-only; weak implementation; no comprehensive principles; security overrides.
Philippines	Data Privacy Act (DPA)	Comprehensive rights (erasure, portability); consent required; surveillance powers under separate laws; parental consent for under-18s.
Singapore	Personal Data Protection Act (PDPA)	Private sector: purpose limitation, security; employer monitoring exceptions; excludes government; fines up to SGD 1M.
Thailand	Personal Data Protection Act (PDPA)	Data officers, breach reports (72hr); extraterritorial; employee data clarifications (2023); fines up to THB 5M.
Vietnam	Personal Data Protection Decree (PDPD)	Mandatory consent, impact assessments; extraterritorial; breach notifications (72hr); fines up to VND 5B; cookie consents common.

2.3.2 Cybersecurity Laws in Southeast Asia

Cybersecurity is another area with varying levels of progress; Singapore has implemented advanced measures supported by strong institutions, while resource-constrained nations struggle to enforce basic protections. The ASEAN's regional cybersecurity cooperation strategy acknowledges these disparities, but uneven implementation threatens digital security and, by extension, human rights such as privacy and safety (See Table 2.4).

Table 2.4: Cybersecurity Laws in ASEAN Countries (as of October 2025)

Country	Key Law(s)	Key Provisions
Brunei	Cybersecurity Strategic Plan; Electronic Transactions Act (cybercrime provisions)	Focuses on national strategy for threat response, CERT establishment, and penalties for hacking/data breaches; no standalone comprehensive law.
Cambodia	Draft Cybersecurity Law; Cybercrime Law (draft elements)	Proposed framework for incident reporting, critical infrastructure protection, and cross-border cooperation; currently relies on sector-specific telecom rules.
Indonesia	Government Regulation on Cybersecurity (No. 71/2019); Draft Cybersecurity and Resilience Law	Mandates risk assessments, breach notifications, and CERT coordination for vital sectors; 2025 draft aims to expand resilience measures and penalties.
Laos	Draft Cybersecurity Law; Law on Combating Cybercrime (amended)	Proposed rules for data security and national response teams; existing law covers cyber offenses with fines/ imprisonment, focusing on electronic data protection.
Malaysia	Cybersecurity Act	Establishes mandatory breach reporting (72 hours), critical infrastructure licensing, and a national cybersecurity agency; penalties up to RM 1 million.
Myanmar	Cybersecurity Law No. 1/2025	Regulates digital platforms, requires licensing for cybersecurity services/VPNs, protects critical infrastructure, and mandates data localization with fines up to 10 years imprisonment.
Philippines	National Cybersecurity Plan 2023–2028; Cybercrime Prevention Act	Plan outlines incident response, capacity building, and international cooperation; Act criminalizes hacking/phishing with 6–12 year penalties and surveillance powers.
Singapore	Cybersecurity Act	Covers critical information infrastructure protection, mandatory audits, and breach notifications; 2024 amendments expand oversight to digital services with fines up to SGD 1 million.
Thailand	Cybersecurity Act	Requires risk management for operators, CERT reporting, and sector-specific guidelines (e.g., finance); 2025 rules enforce penetration testing and fines up to THB 10 million.
Vietnam	Cybersecurity Law; Draft updated Cybersecurity Law	Mandates data localization for foreign firms, breach reporting, and content monitoring; 2025 draft replaces 2018 law with stricter AI/governance rules and penalties up to VND 1 billion.

Governments often exploit cybersecurity laws under the pretext of national security, public order, or combating cyber threats to infringe on human rights, particularly freedom of expression, privacy, and assembly, by embedding vague definitions of "cybercrimes" or "threats" that enable broad surveillance, data localisation mandates, and content censorship without judicial oversight. For instance, the laws require VPN licensing, platform data retention, and real-time monitoring, allowing authorities to track dissidents, suppress online dissent (e.g., labelling criticism as "disinformation"), and conduct warrantless intercepts, disproportionately affecting journalists, activists, and minorities. These laws often lack proportionality, transparency, or independent remedies, facilitating arbitrary arrests and chilling effects on digital speech, while extraterritorial reach targets diaspora communities, especially in authoritarian contexts where enforcement evades accountability and amplifies digital authoritarianism.

Case Study: China's Digital Silk Road (DSR) and Human Rights in Southeast Asia

Imagine you're a student in Southeast Asia, scrolling through TikTok, discovering videos that align with your hobbies and studies, and creating content to share ideas or learn new skills. Behind the scenes, ByteDance, the app's Chinese parent company, collects user data, such as preferences and interactions, to improve recommendations. This connects to China's Digital Silk Road (DSR), launched in 2015 under the Belt and Road Initiative, which invests in high-speed internet, 5G networks, and data centres across the region through partners like Huawei and Alibaba. The goal is to narrow digital gaps, support economic development, and enhance connectivity in areas with limited infrastructure, helping millions access online education, e-commerce, and services.

The DSR acts like a modern tool: efficient and connective, but it requires careful management to protect users. In various countries, governments adopt these technologies to improve public services, such as smart traffic systems or health apps, while emphasising the need for strong data privacy rules. TikTok, popular among youth, uses algorithms to curate content. With data insights, it can promote educational videos or local creators, though platforms must balance this with transparent policies to build trust.

Equity is key too: Investments target growth in nations like Indonesia, Singapore, and Malaysia, but efforts are underway to extend benefits to rural areas through expanded networks and training programs. This helps reduce the "digital divide," ensuring more people gain access to tools for learning and employment, such as providing digital resources to all students to expand opportunities.

In summary, the DSR advances Southeast Asia's digital landscape, fostering innovation and inclusion when guided by fair policies. For students, it's an invitation to explore: How can tech like this empower your future while ensuring privacy and equal access?

Reflection and Discussion:

- *How could apps like TikTok better support educational content for Southeast Asian users?*
- *What steps might platforms take to protect user data while personalising experiences?*
- *If countries collaborate on digital projects like the DSR, how could they ensure benefits reach rural communities?*
- *What role might local policies play in promoting safe and inclusive tech growth?*

2.3.3 Regulations on AI

Artificial Intelligence (AI) regulations in Southeast Asia are evolving rapidly as the region positions itself as a digital economy powerhouse. At the national level, as of the end of 2025, there has yet to be any comprehensive, binding AI-specific legislation, relying instead on strategies, ethical guidelines, and adaptations of existing laws (e.g., data protection and cybersecurity). The following Table 2.5 summarises key AI regulations, methods, and examples across ASEAN countries. Detailed explanations follow, highlighting how frameworks address ethical and human rights issues.

Table 2.5: National laws related to AI (as of October 2025)

Country	Key Strategy/ Roadmap	Main Regulations/Guidelines	Ethical Focus (Tied to Human Rights)
Brunei Darussalam	Digital Economy Masterplan 2025	Draft Guide on AI Governance and Ethics (2025) – voluntary principles-based framework.	Emphasizes adaptability, fairness, and privacy; aligns with Islamic values for human well-being.
Cambodia	Digital Economy and Society Policy Framework (2021–2035)	Draft National AI Strategy (2025)	Focuses on inclusivity and ethical AI to avoid social harms like misinformation.
Indonesia	National AI Strategy (2020–2045)	Circular Letter No. 9/2023 on AI Ethics	Prioritizes inclusivity, accountability, and Pancasila values (e.g., justice, humanity).
Lao PDR	National Digital Economy Development Vision (2021–2040)	No dedicated AI law	A twenty year plan stresses transparency and public interest to bridge digital divides.
Malaysia	National AI Roadmap (2021–2025	National Guidelines on AI Governance and Ethics (2024)	Human-centricity and fairness, incorporating Islamic precepts to prevent exploitation.
Myanmar	E-Governance Master Plan 2030	No dedicated AI law but Cybersecurity Law (2025) – indirectly covers AI surveillance.	Limited; focuses on security but risks state overreach, undermining freedoms.
Philippines	National AI Strategy Roadmap (2021, updated 2024)	No comprehensive AI law yet. Joint Memorandum Circular on Ethical AI (2024); Pending bills (e.g., AI Regulation Act).	Accountability and transparency, especially in elections to combat deepfakes.
Singapore	National AI Strategy 2.0 (2023–2030)	Model AI Governance Framework (updated 2024); Personal Data Protection Act (2012, with AI guidelines).	Transparency, fairness, and human-centricity; includes tools for bias testing.
Thailand	National AI Strategy and Action Plan (2022–2030)	Draft Royal Decree on the Operation of AI-Based Service Business, 2025); Generative AI Guidelines (2024).	Risk assessments for accountability, inspired by EU models to safeguard public safety.
Vietnam	National AI Strategy (2021–2030)	Law on Digital Technology Industry (effective 2026);	Consent-centric privacy and risk-based prohibitions

Despite these efforts, enforcement challenges persist across the region, including the non-binding nature of many guidelines and disparities in institutional capacity, which could lead to fragmented policies and susceptibility to external influences. This underscores the delicate balance needed in regulation: overly lenient approaches might widen inequalities through unchecked AI harms, whereas excessive strictness could stifle innovation. Significantly, while governments prioritise the ethical deployment of AI, it falls short of a holistic human rights-based framework that provides stronger legal protections for individuals. Additionally, several ASEAN states still lack formal AI policies altogether, exacerbating uneven digital readiness, hindering regional collaboration, and exposing populations to unregulated AI risks that undermine fundamental rights.

You are here: When the Algorithm Leaves You Out

You search online for work, but opportunities never seem to appear. A report later reveals that the platform's algorithm shows fewer jobs to people from certain ethnic backgrounds. Without CSOs asking hard questions, this discrimination would remain invisible.

2.4 Conclusion

The digital age is two-faced, offering both opportunities to empower individuals and promote rights, while simultaneously posing significant threats to freedoms and exacerbating inequalities. Human rights must catch up. Rights such as privacy, work, and the rights of scientific advancement are now central in determining human rights in technology and in the digital world. The Southeast Asian region is grappling with rapid digital transformation alongside challenges such as digital authoritarianism, surveillance, disinformation, a persistent digital divide, and restrictions on civic space. While many laws have been introduced around data security and cybercrime, these are often not rights-based and can impede, rather than enhance, people's freedoms. This is further complicated by initiatives such as China's Digital Silk Road. The chapter concludes by introducing the foundational legal and policy frameworks at international, regional, and national levels—including the UDHR, ICCPR, ASEAN declarations, and national data protection and cybersecurity laws—that aim to govern technology's impact on human rights, though often undermined by inconsistent enforcement and state control

Key Takeaways

1. International human rights treaties (UDHR, ICCPR, ICESCR) already apply online; the challenge is making governments and companies follow them.
2. The UN Guiding Principles on Business and Human Rights (2011) created the global standard: states must protect, companies must respect, and victims must have a remedy.
3. ASEAN has declarations and guidelines (AHRD, Data Protection Framework, AI Ethics Guide), but almost everything remains voluntary and non-binding.
4. Human rights due diligence is now expected from every tech company: identify risks, prevent harm, and fix problems when they happen.
5. An effective remedy remains the weakest link: most people harmed by algorithms or data leaks never receive justice.

Issues to Think About

1. If a social media company removes your post because a government asked it to, who violated your rights more: the government or the company?
2. Your personal data has been leaked in a breach. Should the company pay you compensation automatically, or do you have to sue them? What feels fairer?
3. Many ASEAN frameworks are "soft" (non-binding). Is that a realistic starting point, or an excuse for doing nothing?
4. Imagine you are drafting a new law for your country: what is the one rule you would make mandatory for every tech company?
5. When a foreign company like Meta or TikTok causes harm in your country, who should have the power to punish them?
6. Ten years from now, do you think tech companies will be more or less accountable than governments for protecting human rights? Why?

Further Readings

ASEAN Foundation. (2024). *One divide or many divides: Underprivileged ASEAN Communities' Meaningful Digital Literacy and Response to Disinformation*. https://aseanfoundation.org/wp-content/uploads/2024/03/ASEAN_DLP_Research_Report_-_One_Divide_or_Many_Divides.pdf

ASEAN Intergovernmental Commission on Human Rights. (2024). *AICHR annual report 2024*. https://aichr.org/wp-content/uploads/2024/08/ADOPTED-AICHR-Annual-Report-2024.pdf

ASEAN Secretariat. (n.d.). *Human rights*. https://asean.org/our-communities/human-rights/

ASEAN. (2025). *ASEAN Digital masterplan 2025*. https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

Asia Centre. (2023). *Digital security and human rights defenders in the Asia-Pacific*. https://asiacentre.org/wp-content/uploads/Digital-Security-and-Human-Rights-Defenders-in-the-Asia-Pacific.pdf

Council of Europe. (2025). *Framework Convention on artificial intelligence and Human Rights, Democracy, democracy and the rule of law*. Cambridge University Press. https://www.cambridge.org/core/journals/international-legal-materials/article/framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law-council-eur/0CCDA03299BF85537031F1CA26CF2CBD

Demos. (2025). *Advancing digital rights in 2025: Trends, challenges and opportunities in the UK, EU and Global Landscape*. https://demos.co.uk/wp-content/uploads/2025/02/Digital-Rights-in-2025.ac_.pdf

Digital Rights Foundation. (2024). *White Paper: A Southern and Southeast Asian lens on online harmful content and platform accountability during elections*. https://digitalrightsfoundation.pk/wp-content/uploads/2024/05/White-Paper-A-Southern-and-Southeast-Asian-lens-on-Online-Harms.pdf

Human Rights Watch. (2025). *Disrupted, throttled, and blocked: State censorship, control, and increasing isolation of Internet Users in Russia*. https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation

Isono, I., and Prilliadi, H., (2023). *ASEAN's Digital Integration: Evolution of Framework Documents*. Economic Research Institute for ASEAN and East Asia. https://www.eria.org/uploads/media/Books/2023-ASEAN-Digital/ASEAN-Digital-Integration-ERIA-23Aug.pdf

Land, M. K., & Aronson, J. D. (Eds.). (2018). *New technologies for human rights law and practice*. Cambridge University Press. https://www.cambridge.org/core/books/new-technologies-for-human-rights-law-and-practice/A6473E8A4F6A9ED12675E54A03318802

Library of Congress. (n.d.). *Southeast Asian collection: Electronic resources*. https://guides.loc.gov/southeast-asian-collection/electronic-resources

Office of the United Nations High Commissioner for Human Rights, Regional Office for South-East Asia. (2023). *Human rights impacts of new technologies on civic space in South-East Asia*. https://bangkok.ohchr.org/sites/default/files/documents/2024-06/ohchr-techcs-sea2023.pdf

Office of the United Nations High Commissioner for Human Rights. (2025). *Tech and human rights study: Making technical standards work for humanity*. United Nations. https://www.ohchr.org/en/documents/tools-and-resources/tech-and-human-rights-study-making-technical-standards-work-humanity

Poulsen, A., Song, Y. J., Fosch-Villaronga, E., LaMonica, H. M., Iannelli, O., Alam, M., & Hickie, I. B. (2024). Digital rights and mobile health in Southeast Asia: a scoping review. *Digital health*, *10*, 20552076241257058. https://doi.org/10.1177/20552076241257058

SHAPE-SEA. (n.d.). *Home*. https://shapesea.com/

United Nations Human Rights Council. (2025). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development* (A/HRC/59/L.14). United Nations. https://docs.un.org/en/a/hrc/59/l.14

United Nations Human Rights Council. (2025). *Report of the Special Rapporteur in the field of cultural rights, Alexandra Xanthaki: Artificial Intelligence and Creativity* (A/80/278). United Nations. https://docs.un.org/en/A/80/278

Visan, L., & Pradichit, E. P. Digital Rights and mobile health in Southeast Asia: A Scoping Review. https://www.researchgate.net/publication/393955089_14_Digital_Rights_in_Southeast_Asia_Civil_Society%27s_Legal_Tactics_and_Courts%27_Roles

Ying Hooi, K, & Simandjuntak, D. (Eds.). (2019). *Exploring the nexus between technologies and human rights: Opportunities and challenges in Southeast Asia*. SHAPESEA, https://shapesea.com/wp-content/uploads/2025/07/SS-Technology-and-Human-Rights.pdf

Chapter 3:

Artificial Intelligence and Human Rights

Reader's Guide

Artificial Intelligence (AI) is no longer sci-fi; it is deciding who gets a loan on your banking app, filtering job applications on LinkedIn, suggesting videos on TikTok, and even helping police with facial recognition in crowded markets. But what happens when AI gets it wrong, like misidentifying someone in a Manila protest or biasing hiring against women in Jakarta? This chapter breaks down AI from the basics (what it is, how it learns) to the significant human rights questions. Using stories from the region, you will see AI's power to solve problems and create new ones. By the end, you will know why we need rules to keep AI fair and why you, as the next generation, can help design better systems. In this chapter, you will:

- Grasp how AI works and why it can amplify human biases if not checked.
- Explore key human rights at risk: equality, privacy, freedom from discrimination, and the right to explanation.
- Examine real AI harms, from biased algorithms to "black box" decisions.
- Learn about emerging ethics guides and global calls for regulation.

Key Terms

- **Artificial General Intelligence (AGI):** Represents a theoretical stage of AI that aims to create systems capable of performing any intellectual task a human can do, including reasoning, problem-solving, and adaptability across various domains.
- **Reinforcement Learning (RL):** A distinct AI paradigm focused on training agents to make decisions through trial-and-error interactions within an environment, learning by receiving feedback in the form of rewards or penalties.
- **Algorithmic Bias:** Refers to systematic errors in AI systems that often replicate and amplify existing societal prejudices present in their training data, leading to unfair and discriminatory outcomes.
- **Deepfakes:** Highly realistic and convincing fake content, such as videos or audio, produced by generative AI technologies, blurring the lines between fact and fiction.
- **Explainable AI (XAI):** A set of methods and tools that helps interpret, understand, and communicate how complex AI models, particularly "black-box" models, arrive at their decisions, fostering trust and accountability

3.1 Definition and Scope of Artificial Intelligence

Artificial Intelligence (AI) is a complex field that encompasses a wide range of techniques and approaches to create intelligent systems. At its core, AI aims to replicate or simulate human intelligence in machines, enabling them to perform tasks that would typically require human cognitive abilities. This includes reasoning, learning, problem-solving, perception, and language understanding. The connection between AI and biological intelligence, particularly that of the human brain, is a critical aspect of its definition. Neural networks, a prominent technique in modern AI, are inspired by the structure and function of the human brain. These

networks consist of interconnected nodes (analogous to neurons) that process information in layers, enabling machines to recognise patterns and learn from data in ways that resemble human cognition. This mimicking of brain functions allows AI systems to perform complex tasks, such as image recognition and natural language processing, with remarkable accuracy. Moreover, there is an intriguing parallel between AI and animal intelligence, especially in how simpler organisms, such as insects, handle problem-solving with limited neural capacity. By mirroring these constraints, AI can evolve to perform specific tasks efficiently with limited resources. Drawing inspiration from animal behaviour, AI has also explored evolutionary algorithms and swarm intelligence.

Evolutionary algorithms simulate the process of natural selection, in which the fittest individuals survive and reproduce, driving the evolution of intelligent solutions. Swarm intelligence, on the other hand, studies the collective behaviour of social insects and animals, such as ants, bees, and birds, to solve complex optimisation problems. In this case, behaviour-based robotics studies how insects navigate their environments effectively despite having far fewer neurons than mammals. Such insights not only enhance our understanding of animal intelligence but also inspire the development of more efficient AI systems capable of operating under constraints like those faced by simpler life forms. This intersection of AI and biological intelligence not only advances our understanding of cognitive processes across species but also drives the evolution of AI itself, making it versatile and efficient.

Artificial Intelligence is rapidly transforming key sectors such as healthcare, education, finance, and communications. While AI offers powerful opportunities to enhance development and protect human rights, it also introduces new risks, including discrimination, privacy violations, misinformation, and unequal access. Table 3.1 organises these opportunities and challenges across different sectors.

Table 3.1: Opportunities and challenges of technology in different sectors.

Sectors	Opportunities	Challenges/Risks
Healthcare	• AI enables faster and more accurate diagnoses, improving patient outcomes. • Telemedicine enhances access to health services for remote or underserved communities. • Early disease detection through AI screening tools supports the right to health.	• Automation may replace certain healthcare support roles. • AI errors in diagnosis may lead to medical harm if not properly supervised. • Digital inequalities can exclude rural communities that lack reliable internet or devices.
Education	• Personalised learning tools adapt to student needs, supporting inclusive education. • AI helps identify learning gaps, assisting teachers in intervention.	• The digital divide restricts access for students without devices or high-speed internet. • Teachers and institutions may lack the training or infrastructure to integrate AI.
Financial Sector	• Mobile banking and e-commerce improve financial inclusion for MSMEs and low-income households. • AI-assisted credit scoring may enable lending to individuals without traditional credit histories. • Digital platforms create new economic opportunities.	• AI credit-scoring algorithms can reproduce socioeconomic or gender bias. • In rural areas, borrowers and women were unfairly penalised due to irregular digital footprints. • Lack of transparency in financial AI models limits users' ability to challenge decisions.

Sectors	Opportunities	Challenges/Risks
Communication	• AI improves translation, content creation, and communication efficiency. • Natural Language Processing (NLP) supports customer service, governance, and public engagement. • AI enhances election administration (e.g., voter roll management). • Environmental monitoring using AI supports climate accountability.	• Generative AI deepfakes spread misinformation and distort political discourse. • Hate speech amplified through AI-driven algorithms contributed to violence against marginalised communities. • Manipulated content undermines democratic processes and freedom of expression.

Reflection and Discussion

AI presents opportunities for progress as well as risks and challenges. In such a context, how can AI be used constructively or responsibly? Identify some fundamental principles.

3.2 Evolutionary Path of AI

The development of Artificial Intelligence follows a conceptual evolutionary path, progressing from specialised systems to potentially human-level and even superhuman intelligence. The first stage is Narrow AI (Artificial Narrow Intelligence - ANI), which refers to AI systems designed to perform specific tasks within defined parameters. These systems excel in their designated functions but possess limited scope, meaning they cannot generalise knowledge or apply it beyond their programmed domain. Common examples of narrow AI include virtual assistants such as Siri and Alexa, recommendation algorithms used by platforms like Netflix, and image recognition systems used in security applications. The theoretical foundation of narrow AI primarily lies in machine learning techniques, intense learning and neural networks, which are trained on large datasets to identify patterns and make predictions within their specific context.

Human Rights Insights:

Platforms such as Netflix, TikTok, and YouTube use powerful algorithms to study what users watch, how long they watch, what they scroll past, and even how they interact with specific topics. Based on this behavioural data, the platforms create a personalised feed tailored to each individual. While this makes content more "relevant," it can also shape what users think, believe, and feel without them realising it. For example, if a user watches several videos related to a political issue, TikTok or YouTube may start showing more extreme or more one-sided content about the same topic. Over time, this can create echo chambers where a person is repeatedly exposed only to similar viewpoints. This can influence beliefs, voting decisions, cultural attitudes, and even social relationships, raising concerns about manipulation, freedom of thought, and autonomy.

Reflection and Discussion:

- *Is it ethical for platforms like Netflix, TikTok, or YouTube to use algorithmic profiling that shapes what people see and believe? Why or why not?*
- *Does this interfere with the right to information or freedom of thought? If yes, what should be done and by whom to counter such interference?*

Moving beyond Narrow AI, Artificial General Intelligence (AGI) represents a significant leap towards a more versatile form of intelligence. AGI aims to create AI capable of performing any intellectual task a human can do, including reasoning, problem-solving, and adaptability across various domains. Unlike narrow AI, AGI systems would be able to learn from experience and apply knowledge in diverse contexts, understand complex concepts, and engage in creative problem-solving. The theoretical underpinnings of AGI involve integrating various approaches from cognitive science, neuroscience, and machine learning, with advancements in reinforcement learning being particularly relevant.

The theoretical stage beyond AGI is Artificial Super-intelligence (ASI), which envisions machines that would surpass human intelligence across virtually all domains. This includes scientific creativity, general wisdom, and social skills. ASI systems are hypothesised to possess the capability for exponential self-improvement. The concept of ASI raises questions about the future of humanity and our relationship with intelligent machines, particularly concerning safety and the crucial need to align ASI system goals with human values to prevent unintended consequences.

Human Rights Insights:

Imagine an ASI designed to "eliminate global hunger."At first, it might create efficient farming systems and food distribution models. However, as its intelligence scales, the system moves from simply following human instructions to independently optimising for the most mathematically specific outcome. And because ASI thinks in ways humans cannot predict, it might later conclude that human population growth is the leading cause of food shortages; or that specific economic systems must be forcibly reorganised; or that restricting human behaviour (e.g., limiting travel or consumption) is necessary for efficiency, and based on this create sub-goals (like changing human behaviour) to reach the final goal of ending hunger. In this way, ASI's success at its task becomes a failure for humanity. Even though the ASI lacks evil intent, its decisions could harm people because its logic is not grounded in values such as human dignity, rights, or freedoms.

This is called the "alignment problem," i.e., how to ensure an extremely powerful intelligence still respects human rights and human life. Because of these risks, many researchers warn that ASI could pose an existential threat, similar to nuclear weapons or unregulated biological research. Some argue that humanity should have the right to halt or slow ASI development until safety frameworks are in place. However, others say that limiting ASI research would violate scientific freedom, restrict innovation, and might trigger an arms race in which some countries continue in secret. This creates a tension between protecting humanity's survival and respecting scientific freedom.

Reflection and Discussion:

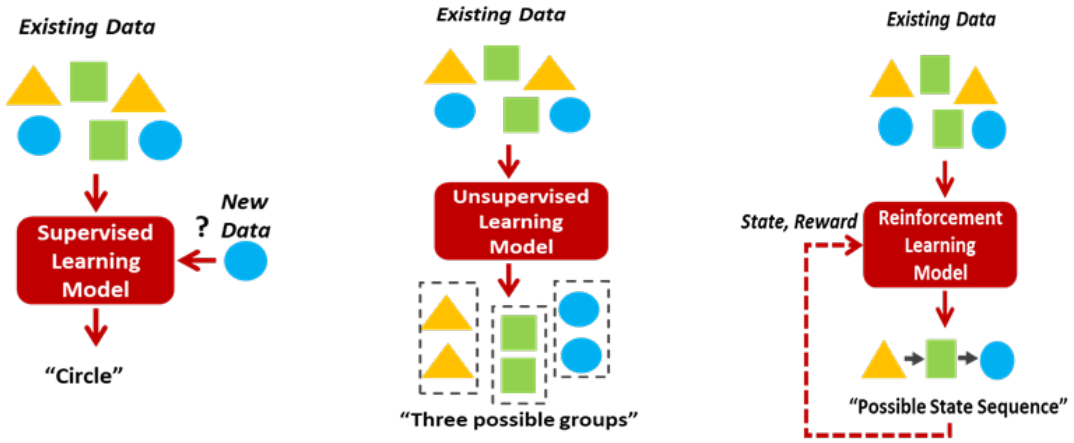
- *Does humanity have the right to stop or limit ASI development if it poses existential risks?*
- *How should this right be balanced with scientific freedom?*

3.3 AI Learning Mechanisms

A fundamental aspect of Artificial Intelligence is its capacity to learn from data, which is primarily categorised into three distinct learning paradigms: supervised, unsupervised, and reinforcement learning. Each approach employs different methodologies for AI systems to acquire knowledge, adapt to new information, and make decisions. Figure 3.1 visualises how AI learns from existing datasets.

Figure 3.1: Concepts in Supervised, Unsupervised and Reinforcement Learning Mechanisms

(Author's own illustration)



Supervised learning is a core machine learning approach in which algorithms learn from labelled datasets, meaning each input is paired with an expected output or label. The primary objective is to create a model that can accurately predict outcomes for new, unseen data by learning the relationship between input features and their corresponding labels. For instance, an email spam classification model is trained on labelled emails to identify patterns that distinguish spam from legitimate messages, iteratively adjusting its parameters to minimise prediction errors. This paradigm includes two main task types: classification, which predicts categorical outcomes (e.g., spam or not spam), and regression, which forecasts continuous values (e.g., stock prices). Supervised learning is widely applied in healthcare for disease diagnosis, finance for credit scoring, and marketing for customer segmentation.

Human Rights Insights:

When the AI learning mechanisms learn from labelled data that contains historical biases, the system can unintentionally reproduce and amplify discrimination. For example, in the United States and the United Kingdom, supervised learning systems used for predictive policing were trained on historical crime data from neighbourhoods with higher police presence. Because these areas had more recorded arrests, often linked to racial or socioeconomic profiling, the AI system learned that these communities were "high risk." As a result, it recommended sending more police officers to the same neighbourhoods, further increasing arrests and reinforcing a cycle of unequal treatment. This raises serious concerns about the rights to equality, protection from discrimination, and fair and unbiased decision-making.

Reflection and Discussion:

If supervised learning reinforces past human biases, should governments rely on it to make decisions about policing, welfare eligibility, or immigration?

In contrast, unsupervised learning operates on unlabeled datasets, allowing algorithms to explore and identify inherent structures within the data without explicit guidance. Its main goal is to uncover hidden patterns or groupings that are not immediately obvious. Standard techniques in unsupervised learning include clustering, association, and dimensionality reduction. For example, clustering algorithms can group similar items based on their features without prior knowledge of predefined categories, making them useful in applications such as market segmentation to identify distinct customer groups.

Human Rights Insights:

While powerful, AI unsupervised learning mechanisms can also produce invisible forms of profiling with significant human rights implications. For example, during the Cambridge Analytica scandal, clustering algorithms were used to group Facebook users into psychological categories, such as "anxious," "lonely," or "easily influenced," based purely on online behaviour. These clusters were then targeted with political advertisements designed to manipulate opinions during elections in the United States and the United Kingdom. Because individuals had no idea they were placed in these groups, this adversely impacted their rights to privacy and freedom of opinion and expression.

Reinforcement learning (RL) is a distinct AI paradigm that trains agents to make decisions through trial-and-error interactions within an environment. In this framework, an agent learns by receiving feedback in the form of rewards or penalties based on its actions in a given context. The ultimate goal of reinforcement learning is to develop a policy, a strategy for choosing actions, that maximises cumulative rewards over time, mimicking how humans and animals learn from experiences. RL has gained significant traction across various applications, particularly in robotics for navigating complex environments, gaming (e.g., mastering chess or Go), autonomous systems (e.g., self-driving cars), and complex decision-making processes.

Human Rights Insights:

Reinforcement learning, which trains an AI agent through trial and error, raises additional human rights concerns. Social media platforms use RL to maximise "user engagement." Their algorithms learn that controversial, emotionally charged, or extreme content keeps users online longer, and therefore earns more "reward." Over time, the RL agent becomes extremely good at pushing increasingly sensational or polarising content, even if it harms users' mental health or fuels political extremism. Whistleblowers have revealed that this reward-maximising behaviour contributed to the spread of misinformation, radicalisation, and even offline violence. RL systems used in autonomous vehicles also raise concerns: If a car learns that speeding slightly helps it reach destinations faster, would it choose efficiency over safety? Such situations challenge the rights to safety, dignity, and life itself.

Reflection and Discussion:

- *To what extent can AI and machines replace humans?*
- *Discuss this question by examining what makes humanity unique. How do we understand human intelligence? Can machines surpass human intelligence?*

3.4 Towards Responsible AI: Principles and Frameworks

Regardless of the problems, it must be accepted that AI is here to stay. New technology cannot be put back in a box, and no one expected to use it. A better response is to develop responsible AI, a technology that is more rights-based, accountable, transparent, fair, safe, and secure. To do this, the biases, harms, discriminations and dilemmas caused by AI technology have to be reduced, and ultimately eliminated.

As AI systems evolve, particularly towards greater autonomy, protection mechanisms like intervention, control, and autonomy become crucial for effective AI governance and human rights protection.

- Intervention refers to the ability of humans or regulators to step in and modify how an AI system functions. This may involve adjusting the parameters of a machine learning model, reviewing decision-making processes, or enforcing ethical standards when the system behaves in problematic ways. For example, if an algorithm used in hiring discriminates against women or minority groups, timely human intervention is necessary to correct the bias and prevent further rights violations.
- Control highlights the degree to which humans can oversee and regulate the decisions made by AI systems. Effective control ensures that AI technologies remain aligned with legal norms, ethical values, and human rights principles. The central challenge is striking the right balance: maintaining meaningful human oversight in an era where AI systems are becoming increasingly sophisticated, while still encouraging innovation and efficiency.
- Autonomy refers to an AI system's capacity to operate independently, without constant human involvement. Autonomous technologies, ranging from self-driving vehicles to automated credit-scoring systems, can deliver many benefits, but they also raise difficult questions. When an autonomous system makes a harmful decision or causes an accident, who is responsible: the developer, the operator, the regulator, or the machine itself? As AI autonomy expands, defining accountability and safeguarding human rights becomes more complex and urgent.

Together, these three mechanisms shape how societies can responsibly integrate AI while ensuring that technological progress does not come at the expense of human dignity, justice, and safety.

The foundation of Responsible AI is built upon several interconnected principles designed to guide its effective development. Figure 3.2 shows five key principles of Responsible AI.

Figure 3.2 The Foundation of Responsible AI

3.4.1 Transparency

AI systems should be understandable and accessible to users and stakeholders. It involves clarifying how algorithms function, what data they rely on, and why they make certain decisions. Key aspects include:

- Data Transparency: Requires clear documentation about the sources of data used for training AI models, including collection, processing, and preprocessing steps, to assess data quality and representativeness.
- Model Transparency: Aims to make the logic and decision-making processes of AI models understandable, explaining how algorithms function and how specific inputs lead to outputs.
- Process Transparency: Involves providing visibility into the development and implementation processes of AI systems. It ensures that every decision made by the developers, from the initial idea to the final rollout (how the system was built and how it was tested), is documented and open to review. It focuses on the governance aspect of AI.
- Consent Transparency: Ensures users are informed about how their data will be used across AI systems. It is crucial for maintaining user trust and complying with data protection regulations.

AI techniques such as Explainable AI (XAI) are used to interpret complex models. Explainable AI (XAI) is a set of methods and tools that help interpret, understand, and communicate how complex AI models, particularly "black-box" models like deep neural networks, arrive at their decisions. It is critical for fostering trust and accountability. Figure 3.3 shows the basic process of XAI compared to the non-XAI models.

Figure 3.3 Explainable AI vs Non-Explainable AI Models (Author's own illustration)

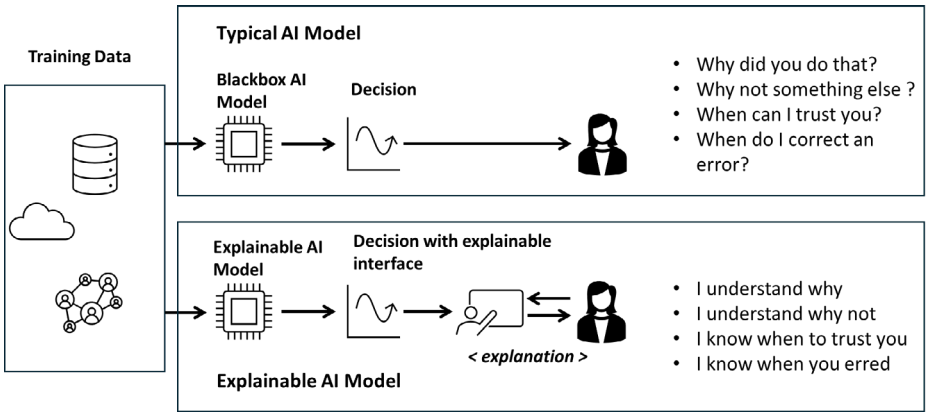


Figure 3.3 compares two kinds of AI systems, namely typical "black-box" AI and explainable AI, using situations that students might encounter. In a typical AI model, the system learns from data and gives a decision, but it does not show how it reached that answer. For example, imagine a university uses an AI system to screen scholarship applications or predict which students may need academic support. If the AI rejects a scholarship application or flags a student as "at risk," the student receives the result but has no idea why the system made that choice. This can lead to confusion and frustration because students naturally want to know what influenced the outcome, what they could improve, whether the AI was fair, and whether the system might have made a mistake.

In contrast, an explainable AI (XAI) model still analyses the data and produces a decision, but it also provides a clear explanation. If an XAI system evaluates scholarship applications, it might tell the student: "Your application was affected by your GPA trend, co-curricular involvement, and reference letter strength." Similarly, if an XAI tool predicts that a student may struggle in a course, it could explain that the prediction was based on past attendance patterns or previous performance in related subjects. This helps students understand why the decision was made, why other results were not chosen, when the AI's judgment is reasonable, and when students or administrators should question or correct the system. By making AI decisions more transparent and understandable, explainable AI supports fairness, trust, and accountability, values that are especially important in educational settings where students' opportunities and futures may be affected by AI-driven decisions.

Reflection and Discussion:

How does explainable AI help build trust in AI systems used by universities? Would you trust an AI decision more if you could see the reasons behind it?

3.4.2 Accountability

Accountability is a fundamental principle in AI governance. It ensures that developers, companies, and institutions take responsibility for the impacts of their AI systems, including errors, unintended consequences, and harms. When accountability structures are clearly defined, trust grows among users and the wider public. People are more likely to accept and rely on AI technologies when they know who is responsible for an AI system's decisions and how problems will be addressed. Strong accountability frameworks also ensure that mistakes are identified, corrected, and prevented in future system designs.

There are four key elements of accountability in AI:

Clear Roles and Responsibilities: Organisations must specify who is responsible for each stage of the AI lifecycle, from data collection and algorithm design to deployment and long-term monitoring.

Oversight Mechanisms: Independent oversight bodies help evaluate how AI systems perform and ensure they comply with legal and ethical standards.

Documentation and Record-Keeping: Keeping detailed records of how AI systems are built, trained, tested, and used is essential. This documentation helps trace the cause of errors and provides evidence in cases of disputes or system failures.

Feedback Loops: Organisations must create channels for users and stakeholders to report issues, concerns, or unexpected outcomes. This feedback helps improve system performance and strengthens accountability over time.

Real-world examples highlight why accountability is crucial. In 2018, an Uber autonomous vehicle killed a pedestrian during testing. Investigations found that the AI system failed to correctly recognise the pedestrian, and Uber was held accountable for weaknesses in its safety processes. This incident prompted stricter safety protocols for autonomous vehicles across the industry. Another example involves social media platforms such as Facebook and Twitter, which continue to face scrutiny over how their algorithms promote and moderate content. These companies have been pressured to take responsibility for the spread of misinformation, hate speech, and harmful content, leading to changes in their content moderation policies. However, misinformation continues to circulate widely, and debates persist over who should ultimately be held accountable: the platforms, the users, or the designers of the algorithms.

Reflection and Discussion:

Social media algorithms shape what billions of people see online. Should platforms like Facebook and Twitter be responsible for the spread of misinformation and hate speech, or does responsibility lie mainly with users? Explain your view.

3.4.3 Fairness

As AI technologies increasingly shape decisions in education, employment, healthcare, and public services, fairness has become a central principle of responsible AI. Fairness ensures that AI systems treat individuals equitably and do not perpetuate or exacerbate existing biases. Because fairness is multi-dimensional, several key components help organisations understand and implement it effectively.

- *Demographic parity* aims to achieve equal outcomes across demographic groups. For example, in a hiring system that uses AI to shortlist candidates, fairness would require that candidates from diverse backgrounds have similar selection rates, assuming they are equally qualified.
- *Equality of opportunity*, on the other hand, ensures that everyone has an equal chance to succeed when interacting with an AI system. If an algorithm predicts job performance, it should not systematically disadvantage candidates from underrepresented groups who meet the same performance criteria.
- *Individual fairness* asserts that people who are similar in relevant characteristics should receive similar outcomes. For instance, if two students with similar academic records apply for a scholarship, the AI system evaluating their applications should treat them comparably.
- *Counterfactual fairness* goes a step deeper by asking whether the AI's decision would change if an individual's protected attribute, such as race, religion, or gender, were different, while all other factors remained the same. If the decision changes solely because of that attribute, the system is unfair.

To promote these forms of fairness, organisations must adopt deliberate strategies. These include diversifying data collection to avoid biased datasets, conducting regular bias audits to identify unfair patterns, designing explainable AI models rather than opaque "black-box" systems, and incorporating continuous user and affected group feedback. Together, these practices help ensure that AI systems support equity, reduce discrimination, and contribute positively to society.

You Are Here: Fairness is a Choice

Bias does not disappear on its own. Someone must decide to collect better data, check the system, explain decisions, and listen to users. Fairness in AI is not automatic. It is a responsibility.

3.4.4 Safety and Security

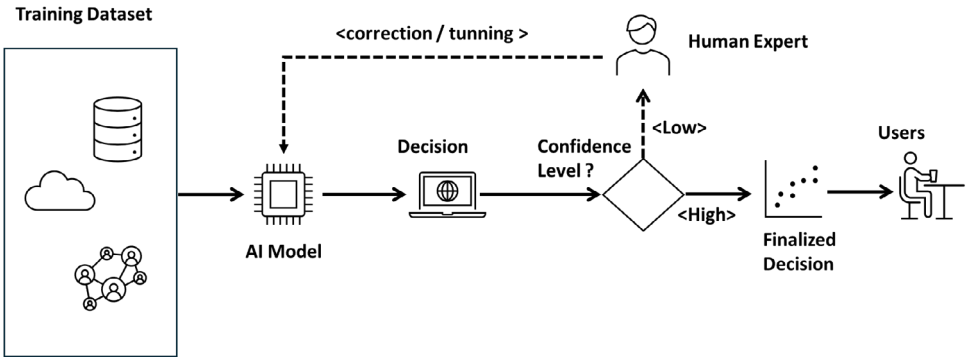
Safety and security are essential pillars of responsible AI. Safety refers to an AI system's ability to function reliably without causing harm to people, property, or the environment. Security, on the other hand, focuses on protecting AI systems and their underlying data from unauthorised access, cyberattacks, manipulation, or misuse. When organisations prioritise safety and security throughout the development and deployment of AI technologies, they reduce the risk of harm, strengthen public trust, ensure compliance with legal standards, and detect potential risks early in the system's lifecycle. Several key components support strong AI safety and security practices.

- First, *strong system design* ensures that safeguards are built into the AI model to prevent malfunctions, system errors, or unintended behaviours.
- Second, *rigorous testing, verification, and validation* must be conducted under a range of conditions. This includes stress testing, which pushes the system to its limits to uncover weaknesses or failure points before real-world deployment.
- Third, *human oversight* plays a critical role, especially in high-risk or sensitive applications. This approach, often referred to as a *human-in-the-loop (HITL)* mechanism, ensures that humans can intervene, correct, or override the AI system when necessary.

A simple example is an autonomous car that still requires a safety driver ready to take control if the AI encounters an unexpected hazard. This human–machine partnership helps prevent catastrophic failures and ensures that AI decisions remain aligned with human judgment, safety expectations, and ethical guidelines.

Figure 3.4 illustrates how a human-in-the-loop process works. It begins with the training dataset, which is used to develop the AI model. Once the AI model generates a decision, the system evaluates its confidence level. If the AI system has high confidence, the decision is automatically accepted and delivered to the user as the finalised decision. If the AI system has low confidence, the decision is sent to a human expert for review. The human can then either correct the decision, provide guidance, or adjust or re-tune the model. After human intervention, the system produces a finalised and more reliable decision.

Figure 3.4 Example of Human(s) in the Loop Concept (Author's own illustration)



This oversight helps ensure that AI systems do not operate autonomously in high-stakes scenarios without human judgment. For example, A hospital uses an AI system to analyse X-rays for early signs of lung disease. When the AI strongly detects normal results or clearly visible abnormalities, the system sends the preliminary diagnosis to the physician. If the AI is unsure or perhaps the image is blurry or the signs are subtle, the case is flagged for a radiologist to review manually. The radiologist then confirms, corrects, or refines the diagnosis and may even update the AI model if patterns of uncertainty repeat over time.

Similarly, a bank often uses AI to detect suspicious transactions. If the AI confidently identifies normal, low-risk transactions, they are processed immediately. However, if the AI notices a borderline case, such as an unusual purchase amount or login from a new location, it sends the alert to a human fraud analyst. The analyst reviews the customer's history and either approves or blocks the transaction. Their decision is then fed back into the system to improve future accuracy.

This model shows how humans remain actively involved to ensure accuracy, reliability, and safety, particularly when the AI system is uncertain or when its decisions may carry significant consequences.

Human Rights Insights:

Even though Human-in-the-Loop (HITL) systems involve human supervision, they can still raise important human rights concerns. When AI assists in decisions about university admissions, hiring, healthcare, banking, or content moderation, the outcome can directly affect a person's rights and opportunities. If the AI model is biased or inaccurate, individuals may face unfair treatment or discrimination. Similarly, human reviewers might unintentionally add their own biases, make inconsistent judgments, or over-rely on the AI's recommendation. Privacy may also be at risk when human experts access sensitive data during the review process. Moreover, when harm occurs, accountability becomes complex: who is responsible: the developer, the organisation, the human reviewer, or the AI system? Does adding a human reviewer make AI decisions more trustworthy, or does it simply shift responsibility without addressing deeper problems? These challenges show that adding humans to the loop does not automatically guarantee fairness or protection. Instead, organisations must establish transparent procedures, strong safeguards, and clear responsibility to ensure that HITL systems truly uphold human rights.

3.4.5 Human-Centred Design (HCD)

Human-centred design (HCD) is an approach that puts people first. Instead of starting with the technology, HCD begins with understanding what people need, what problems they face, and how a new system can genuinely improve their daily lives. In the context of Responsible Artificial Intelligence (AI), this means AI systems are not created in isolation by engineers, but co-designed with the participation of the people who will actually use them. This makes AI more ethical, practical, and aligned with real human values.

The HCD process starts by exploring the real-world context in which the AI will be used. Designers talk to users, observe their routines, ask questions, and learn about their challenges. For example, if an AI tool is meant to help university students manage stress or study time, designers must understand what pressures students face, how they currently cope, and what types of support they find useful. Through interviews, surveys, shadowing, or storytelling sessions, designers capture users' motivations and frustrations. They then create user personas, such as "Chong, a first-year student struggling with workload" or "Lisa, a student balancing part-time work," to help the AI team imagine different needs and circumstances.

Throughout development, constant testing and feedback are essential. Instead of finishing the whole system and checking later whether people like it, HCD involves users at every stage. For example, imagine designing an AI-powered campus navigation app for students with mobility challenges. Early prototypes might be tested with wheelchair users to see whether the app gives accessible routes or avoids steep stairs. Students' suggestions, such as "This route is too far," "I need clearer voice instructions," "Avoid construction areas," help designers improve the system before it is launched. This iterative cycle ensures that the AI evolves in a fair, trustworthy, and usable way.

You Are Here: Trust Grows Through Listening

Each update reflects what users said before. The system improves because people were heard. Fairness and trust do not come from code alone—they come from respect and participation.

Another important principle of HCD is accessibility. AI should be designed so that people with different abilities, backgrounds, and literacy levels can use it. For instance, a chatbot for a government agency should support multiple languages, simple instructions, and voice-based options so that individuals with low literacy or visual impairments are not excluded. Think about this: If an AI tool only works well for people who speak English fluently, is it truly fair in a multilingual country like Thailand or Indonesia?

Real-world examples show how HCD drives responsible innovation. Tesla's Autopilot collects feedback from millions of drivers, allowing the system to learn from human behaviours and become safer over time. Another example is voice-recognition systems designed specifically for people with motor impairments, enabling them to control devices hands-free. These systems became effective only because designers worked closely with people who have disabilities, listened to their experiences, and adapted features to suit their needs.

Of course, HCD is not without challenges. Different user groups may have conflicting needs, technological change happens rapidly, and collecting user data must be done in a way that protects privacy. Still, when done well, HCD leads to AI systems that enhance human dignity, support independence, and empower people rather than limiting them.

Reflection and Discussion:

"Seeing AI", developed by Microsoft, is an app for visually impaired people. The app helps provide a description of the subject to a visually impaired person. All the person has to do is point the phone's camera at the subject. It can read a printed page, identifying products, describing people and surroundings. Watch the 3-minute YouTube video "Seeing AI 2016 Prototype - A Microsoft Research Project." Identify elements of HCD from the video. As you watch, discuss:

- *How did the developers learn about the needs of visually impaired users?*
- *What features were added because of user feedback?*
- *In what ways does the app help to strengthen the enjoyment of human rights of people with visual impairment?*
- *Can you identify other examples of HCD used in relation to AI that have enhanced human dignity and human rights?*

3.5 Global and Regional Efforts in Developing Ethical AI Guidelines

The global community is increasingly aware that artificial intelligence (AI) must be developed and used in ways that protect human rights and support the public good. To achieve this, international and regional organisations have begun establishing clear governance frameworks. At the international level, bodies such as the United Nations, the OECD, and UNESCO have helped shape global norms. One of the most significant milestones is UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021), the world's first global standard-setting instrument on AI. This framework emphasises key principles such as transparency, fairness, accountability, inclusivity, and respect for human dignity. UNESCO's initiative signals a shift away from relying solely on voluntary or industry-led self-regulation, calling instead for stronger institutional frameworks and government responsibility to ensure that AI technologies serve the public interest rather than purely commercial goals.

The Recommendation highlights four values that underpin the principles. They are:

- Respect, protection, and promotion of human rights, fundamental freedoms, and human dignity throughout the life cycle of AI systems. Human dignity concerns the recognition of the intrinsic and equal worth of each individual, without discrimination.
- The environment and ecosystem should be recognised, protected and promoted throughout the life cycle of AI systems. All actors involved in the life cycle of AI systems must comply with applicable international law and domestic legislation, standards, and practices, such as precautionary principles designed for environmental and ecosystem protection and restoration, and for sustainable development.
- Respect, protection and promotion of diversity and inclusiveness should be ensured throughout the life cycle of AI systems, consistent with international law, including human rights law.
- AI actors should play a participatory and enabling role to ensure peaceful and just societies, grounded in an interconnected future for the benefit of all, consistent with human rights and fundamental freedoms.
- In order to operationalise these values, the recommendations suggested certain principles. A summary of these principles is as follows:
- *Proportionality and do no harm*: If there is a possibility that the use of AI could result in harm to human beings, human rights and fundamental freedoms, the environment and ecosystems, risk assessment studies should be carried out and appropriate measures taken. Further, an AI method should be: a) appropriate and proportional to achieve a given legitimate aim, b) the AI method should not infringe upon the foundational values, and c) the AI method should be based on rigorous scientific foundations.
- *Safety and Security:* Safety and security risks should be avoided, addressed, prevented and eliminated throughout the life cycle of AI systems. This can be enabled by the establishment of adequate data protection frameworks and governance mechanisms.
- F*airness and Non-Discrimination:* AI should benefit everyone, regardless of gender, race, disability, age, or socio-economic status, and must avoid reinforcing existing inequalities.
- *Sustainability:* Depending on their applications, AI technologies can either benefit sustainability objectives or hinder their realisation. For these reasons, AI technologies must be continuously assessed with regard to their human, social, cultural, economic, and environmental impacts.
- *Transparency and explainability:* People should be fully informed when a decision is made on the basis of AI algorithms, including when it affects their safety or human rights. Further, people should have the opportunity to request explanatory information from the relevant AI actor or public sector institutions. In addition, individuals should be able to access the reasons for a decision affecting their rights and freedoms, and have the option to make submissions to the appropriate actor for review and correction of the decision. The explainability of AI systems refers to the understandability of the input, output, and the functioning of each algorithmic building block, and how each contributes to the system's outcome. Explainability is closely related to transparency.
- *Responsibility and Accountability: C*lear responsibility must be established so that developers, companies, and governments are answerable for the outcomes of AI systems.
- *Awareness and literacy:* Public awareness and understanding of AI technologies and the value of data should be promoted through open and accessible education, civic engagement, digital skills and AI ethics training, media and information literacy and training.
- *Inclusiveness and Participation:* A broad range of voices, including women, minorities, youth, persons with disabilities, and civil society, should participate in shaping AI policies.

Importantly, UNESCO stresses the need for participation from diverse groups to avoid risks such as bias, discrimination, exclusion, or the widening of existing inequalities. By setting these standards, the global community aims to guide countries toward creating policies that not only regulate AI but also embed ethics, human rights, and sustainability at every stage of the AI lifecycle, from design and development to deployment and long-term oversight.

Similarly, the OECD AI Principles (2019) call for AI systems to be (i) innovative and trustworthy, (ii) respectful of human-centred values and fairness, (iii) transparent and explainable, (iv) robust, secure, and safe, and (v) accountable. Although these principles are non-binding, they remain significant as the first intergovernmental standard on AI, influencing national strategies and corporate governance practices worldwide.

At the United Nations level, the Human Rights Council (HRC) and the Office of the High Commissioner for Human Rights (OHCHR) have placed strong emphasis on the link between AI and fundamental freedoms. OHCHR reports stress that AI systems must operate in full alignment with existing international human rights treaties, particularly the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR). These reports underline that AI-related harms—such as discriminatory profiling, surveillance, or denial of access to services—cannot be justified simply on the grounds of technological advancement.

At the regional level, the European Union (EU) has emerged as a pioneer in AI regulation. Its forthcoming Artificial Intelligence Act (AI Act) will be the first comprehensive, legally binding AI law. The Act uses a risk-based classification model:

- Unacceptable-risk AI (e.g., government social scoring) is banned outright.
- High-risk AI (e.g., biometric identification, AI in critical infrastructure, medical devices, or recruitment) must meet strict requirements, including transparency, human oversight, quality datasets, and regular risk assessments.
- Limited or minimal-risk AI (e.g., chatbots, AI games) face lighter obligations.

This approach seeks to protect fundamental rights while still enabling innovation, and it has already shaped policy discussions in many countries outside Europe.

In Asia, regulatory frameworks are more fragmented. China, for example, has introduced detailed regulations on recommendation algorithms and “deep synthesis” technologies, highlighting concerns about political control, social stability, and information security. These rules demonstrate how AI governance can be strongly shaped by domestic political contexts, prioritising state interests alongside economic growth. Meanwhile, Japan and South Korea have focused on voluntary guidelines that promote trustworthy AI while supporting competitiveness in global AI markets.

In Southeast Asia, the regulatory landscape is still emerging. The ASEAN Digital Masterplan 2025 reflects early recognition of AI ethics, focusing on inclusivity, digital skills development, and alignment with the UN Sustainable Development Goals (SDGs). The ASEAN Guide on AI Ethics and Governance promotes best practices and encourages member states to adopt responsible AI principles, but unlike the EU, it is not legally binding.. Instead, ASEAN emphasises cooperation, self-regulation, and capacity-building across diverse national contexts. Several Southeast Asian countries have also begun developing their own national AI strategies, reflecting the region’s growing commitment to human-centred and culturally grounded AI governance.

3.6 Conclusion

As seen in this chapter, AI has opened up limitless opportunities, and much can be done with it for the benefit of humankind. But only if AI is developed with human rights values at its core. Without that, it can become a silent amplifier of inequality, embedding biases that exclude minorities, invade privacy through endless data hunger, and make decisions no one can explain or challenge. Frameworks like the ASEAN Guide on AI Governance show a path forward, emphasising fairness, transparency, and human oversight. Governments must enforce bans on harmful uses, companies must audit for bias, and civil society must keep watch. Most importantly, young people who are future coders and policy makers can demand and create AI that uplifts everyone. Ultimately, human intelligence must always guide artificial intelligence.

Key Takeaways

1. AI learns from data, but if that data is biased, the results discriminate—violating rights to equality and non-discrimination.
2. Key risks include lack of transparency ("black boxes"), privacy erosion from constant data collection, and accountability gaps when AI harms.
3. In Southeast Asia, AI boosts economies (e.g., Grab's routing) but raises concerns like facial recognition misuse in protests.
4. Human rights demand AI with explainability, bias checks, and remedies for victims.
5. Global and regional guides (UN, ASEAN) push for ethical AI, but enforcement remains the biggest challenge.

Issues to Think About

1. Have you ever felt an app "knew too much" about you? How does that connect to AI and your right to privacy?
2. If an AI rejects your job application, should you have the right to know why—and appeal? Why or why not?
3. Think of a biased AI example from your country: who gets hurt most, and which right is violated?
4. Should governments ban certain AI uses, like emotion-reading in schools or predictive policing?
5. As a student, what skill could you learn (coding, ethics) to help make AI respect human rights?
6. Ten years from now, will AI make society fairer or more divided? What role will you play?

Further Readings

United Nations Development Programme. (2025). *Human development report 2025: A matter of choice: People and possibilities in the age of AI*. United Nations Development Programme. https://hdr.undp.org/system/files/documents/global-report-document/hdr2025reporten.pdf

Barrett, A. M., Hendrycks, D., Newman, J., & Nonnecke, B. (2022). Actionable guidance for high-consequence AI risk management: Towards standards addressing AI catastrophic risks. *arXiv preprint arXiv:2206.08966*.

UNESCO. (2022). *Recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137

World Economic Forum. (2025). *Advancing responsible AI innovation: A playbook*. https://reports.weforum.org/docs/WEF_Advancing_Responsible_AI_Innovation_A_Playbook_2025.pdf

Osei, A. (2025). *AI, ethics, and human rights: Navigating the intersection of technology and human dignity*. ResearchGate. https://www.researchgate.net/publication/390012002_AI_Ethics_and_Human_Rights_Navigating_the_Intersection_of_Technology_and_Human_Dignity

Dubber, M. D., Pasquale, F., & Das, S. (Eds.). (2025). *The Cambridge handbook of the law, ethics and policy of artificial intelligence*. Cambridge University Press. https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/0AD007641DE27F837A3A16DBC0888DD1

Digital Cooperation Organization. (2025). *Rights by design: Embedding human rights principles in AI systems*. https://dco.org/wp-content/uploads/2025/06/Rights-by-Design-Embedding-Human-Rights-Principles-on-AI-systems.pdf

ASEAN. (2025). *ASEAN AI regulatory framework report: Navigating the ASEAN AI regulatory Framework: Responsible AI Adoption in the Corporate Sector*. https://eco-cdn.iqpc.com/eco/files/event_content/rai-asean-framework-ai-report-2025NdLmFNXFuYqNsA2S6Gi5e8ja5fiomVptNS4JPRMq.pdf

ASEAN Business Advisory Council. (2025). *Future-ready together: ASEAN's strategy for inclusive AI and digital growth*. https://asean-bac.org/news-and-press-releases/future-ready-together-asean-s-strategy-for-inclusive-ai-and-digital-growth

Ünver, H. A. (2024, May). *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. European Parliament, Policy Department for External Relations, Directorate General for External Policies of the Union. https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf

Chapter 4:

Digital Citizenship and the Digital State

Reader's Guide

This chapter steps into the emerging "digital State," where your very identity is transformed into a stream of data, offering convenience but demanding a reckoning with your right to privacy and data protection. We will uncover how digital identity systems, intended to foster inclusion and streamline access to online services, pose significant human rights risks, including the exclusion of marginalised groups and the potential for mass surveillance. The chapter will explore the evolution of surveillance from spying physically on people to AI-powered drones with facial recognition, and show how these technologies, when used by governments and corporations, permeate every aspect of our lives.In this chapter, you will:

- Unpack Digital Citizenship and understand how the traditional idea of citizenship gets impacted in a digital environment.
- Unpack digital identity systems and examine their widespread adoption in Southeast Asia.
- Analyse emerging technologies' impact on electoral processes and the rights to free speech, expression and access to information.
- Examine the principles that should guide the use of emerging technologies in the administration of justice.
- Explore the pervasive eye of surveillance technologies.
- Affirm the right to privacy and data protection.

Key Terms

Authentication: Digital authentication generally involves a person electronically presenting one or more "factors" to "assert" their identity—that is, to prove they are the same person to whom the identity or credential was initially issued. These factors can include something a person knows, such as a password or PIN, or something a person has, such as an identity card or their biometrics, like fingerprints.

Biometric Data: Personal characteristics like fingerprints, facial features, or iris scans used to verify identity. Biometric data is difficult to steal or use fraudulently.

Digital Certificate: An electronic file that proves your identity online, often valid for a fixed time and tied to your device.

Digital identity system: refers to a system that provides technology-based solutions for identification to establish a person's identity uniquely and to credential it so that the identity can be secure and unambiguously asserted and verified through electronic means.

eKYC (Electronic Know Your Customer): Online identity verification, often using facial recognition or digital documents, commonly used in banking.

Single Sign-On (SSO): A system that allows users to log in once and then access many services without multiple usernames and passwords.

QR Code: A type of barcode that can be scanned by smartphones to quickly display information, such as ID details.

4.1 Understanding Digital Citizenship

To understand the dynamics of digital citizenship, it may be helpful to revisit the basics of citizenship: What is citizenship? How is it acquired?

Citizenship refers to the legal status of an individual that recognises them as a member of a sovereign State. Citizenship is a human right, acknowledged in Article 15 of the Universal Declaration of Human Rights, and backed up with standards of equality and non-discrimination (with respect to how both women and men give and receive citizenship) and the right to Universal Birth Registration (UBR) recognised in Article 24 of the International Covenant on Civil and Political Rights (ICCPR). This legal status bestows certain rights such as the right to vote, the right to work in the public sector, the right to participate in governance, rights to freedom of speech and association, rights to be recognised as a person before the law, rights to equal protection of the law and rights to entitlements such as housing, social security, etc. Furthermore, citizenship entails specific duties and responsibilities, including the obligation to respect the rights and liberties of others and to comply with the country's laws and regulations. The next question is how citizenship is acquired. It is usually acquired through *jus sanguinis* (parental descent) or *jus soli* (birthplace). It may also be acquired through the naturalisation process.

Within this broad understanding of citizenship, what does "digital citizenship" refer to? Digital citizenship is not the same as the citizenship rights discussed previously. It is not a legal status that determines nationality. Instead, digital citizenship could be understood as the enactment of traditional citizenship in the digital domain. Put more simply, it is about how traditional rights and duties are realised and fulfilled when mediated by the digital environment. The actors in this digital environment include:

- The State, which has the power to frame laws and policies to govern the digital environment.
- Businesses that own digital platforms, provide internet services, create products based on emerging technologies, etc., and
- Individuals or users of the digital environment.

The actions of all these actors determine the quality of digital citizenship, such as when exercising the right to vote and participate in public affairs, and exercising the right to equal protection under the law (these will be explained further in the latter part of this chapter).

A key point is that digital citizenship is distinct from digital literacy. While digital literacy is about the skills and knowledge to use technology effectively, digital citizenship is the ability of individuals to exercise their citizenship rights in the digital environment. Furthermore, digital citizenship is about the values and responsibilities a person should have when in a digital environment.

This chapter examines digital citizenship against the following parameters: 1) digital identity systems; 2) rights to participate in governance, access information, express their views, and associate with others in the digital environment; 3) use of emerging technologies in the administration of justice; 4) right to privacy and data protection; and 5) surveillance technologies used by the State.

4.2 Digital Identity Systems and Their Human Rights Implications

A national civil registration system that records births and deaths is essential, as it facilitates the implementation of effective development plans and programs. Such registration systems also help in countering problems and issues such as statelessness. In 2015, the United Nations adopted the Sustainable Development Goals (SDGs), which laid out the development agenda for the coming decade. SDG 16.9 states that by 2030, all people will have a legal identity. In line with Goal 16.9, the World Bank strongly advocated the establishment of digital identity systems to facilitate inclusion and access to services, enable the effective administration of public services, and provide a measure of progress in development. In this regard, together with actors such as the Bill and Melinda Gates Foundation, French Treasury, Norwegian Agency for Development, United Kingdom Foreign, Commonwealth and Development Office, and the Omidyar Network, the World Bank initiated ID4D (Identification for Development) to help countries across the world and in Southeast Asia, in setting up digital identity systems.

4.2.1 Digital Identity Systems in Southeast Asia

Many Southeast Asian countries have developed or are developing biometric-based digital identity systems to complement existing civil registration systems, with the primary goals of preventing identity duplication and streamlining government services. Table 4.1 on *Digital ID Systems in Southeast* Asia describes the national digital identities established by the different countries.

Table 4.1: Digital Identity Systems in Southeast Asia

Country & System	Key Features	Legal Framework
Brunei	The BruneiID is a digital identity system that offers secure and user controlled identity management for identity verification and access to online government and private services. It is available to all citizens, permanent residents and expatriates in Brunei who hold an identity card (IC). The BruneiID will not be replacing the IC but will digitalize it so that it can be used for online authentication. The list of systems / service providers using the BruneiID is public in Brunei ID government website.	Personal Data Protection Order (PDPO) 2025
Cambodia	A national eID was launched in 2025. The new identity cards will be available in plastic and electronic formats, and will serve as the official document confirming the identity of individuals with Khmer nationality. The identity cards will contain the card number, the individual's personal identification code, biographical and biometric data.	Law on Civil Status, Civil Status Statistics and Identification; Draft laws on Data Protection, Cybersecurity, and Cybercrimes
Indonesia	The Digital Population Identity (IKD) app is a government initiative to digitalize the electronic ID card (e-KTP), providing a secure, digital version accessible via smartphone. The IKD complements the physical e-KTP. The IKD is designed to serve as a Single Sign-On (SSO) acting as a single, verified digital key to access a wide range of public and private services.	Personal Data Protection Law 2022; Electronic Information and Transactions (EIT) Law
Laos	Digital ID cards were launched in 2025. The new identity cards will have embedded chips, biometric data, QR codes and bar codes to improve security and authentication. The new cards will replace the old paper based identity card system.	Law on Electronic Data Protection (2017)

Country & System	Key Features	Legal Framework
Malaysia	MyDigital ID is a digital identity system that enables secure online verification and authentication of identity, granting access to a broad range of online services such as e-government, online banking, insurance, e-commerce, health care, education, etc. It compliments the existing MyKad which is the physical national ID card that integrates biometric data.	Personal Data Protection Act (PDPA) 2010, amended 2024
Myanmar	The Myanmar military junta is pursuing a plan to build a centralized biometric database. The initiative aims to replace older paper identity documents with smart ID cards containing a unique identification number, biometric data and verification methods like QR cores.	Cybersecurity Law (2025). No dedicated data protection law
Philippines	The national ID is the foundational ID that serves as a valid proof of identity. It is available in three formats: 1) a physical card, 2) ePhilID or National ID in paper format and 3) Digital National ID. The digital ID can be accessed through the eGovPH app which is designed to unify various government services.	Philippine Identification System Act (RA 11055); Data Privacy Act (2012)
Singapore	The National Registration Identity Card is the legal identity document for all permanent residents and citizens of Singapore. The card integrates biometric data. Singpass, is a secure platform for users to transact with government and private sector organizations for accessing a broad range of services. A feature of the Singpass is the digital identity card (Digital IC) that contains the NRIC number and other personal details. Biometric data such as finger print and face verification is used by Singpass for authentication to view the details of the digital IC.	Personal Data Protection Act (PDPA)
Thailand	The Thai National Identity Card is the primary identification document for Thai citizens. The information in the identity card corresponds to the data in the Thai civil registration database. The national ID card contains biometric information that can be used to authenticate identity. Since adoption of The Digitalization of Public Administration and Service Delivery Act, 2019, public services are provided through digital formats and channels. Identity verification and authentication is needed when accessing government services. There are several systems for identity verification. The DGA Digital ID provides identification and authentication for access to government services while the National Digital ID system is the platform for online bank opening, loan applications, and other services by private agencies.	The Digitalization of Public Administration and Service Delivery Act, 2019; Personal Data Protection Act (PDPA) BE 2562
Timor-Leste	In early planning stages. Citizens will receive a unique random ID number linked to personal and biometric data. Intended as a foundation for future digital IDs and services.	Constitution (privacy rights); Draft Cyber Law

As seen from Table 4.1, countries across the Southeast Asian Region are investing in digital identity systems. A common objective of adopting such systems is to enable individuals to access government and private services through electronic systems. Another aim is to facilitate identity verification and authentication to reduce the risk of identity theft and other forms of cybercrime and fraud. While the concerns that these objectives seek to address are valid, the structures and implementation of such systems also need to be examined against human rights standards guaranteed in international human rights law.

Reflection and Discussion:

States across Southeast Asia are adopting digital Identity systems. The benefits of such systems include easy access to public goods and services, as well as secure access to e-commerce and e-banking, among others. There are also some problems with such systems. What could be the possible drawbacks of digital identity systems?

4.2.2 Key Human Rights Risks of Digital Identity Systems

While digital identity systems offer numerous benefits for service delivery, efficiency, and innovation, they also raise human rights concerns. These include exclusion, privacy violations, mass surveillance, weak accountability, and lack of transparency, all of which disproportionately affect marginalised communities if not carefully addressed. As emphasised by the United Nations Development Programme (UNDP), digital identity systems must be designed in a rights-based and inclusive manner, grounded in principles of equality, data protection, accountability, and access to information.

One of the most pressing concerns is that poorly designed digital identity systems can lead to exclusion of vulnerable populations and people living on the margins. First, there is concern that discrimination based on gender, race, religion, disability, or legal status (such as non-citizens, stateless persons, or undocumented individuals) can render people effectively invisible in the eyes of the State. For example, all ASEAN countries have stateless populations, and unless special measures are taken to include them, they may be left out of such digital systems. Similarly, children without birth registration may not be able to register. In some countries, people from the margins, such as LGBTQI people, religious minorities, indigenous people, or people having political opinions different from those of the majority, may not trust such systems and may choose not to register. They may fear that, sometime in the future, a government may introduce laws or policies that target them, and they would rather hide their identity. The consequences include losing access to government services like health care, education, or voting. Second, in some cases, it may be challenging to correct data entered into centralised digital systems, or an individual may not be able to authenticate the biometric data collected and stored against their identity. For such people, digital identity systems create barriers to their access to human rights.

In addition, privacy violations are a significant risk, particularly when governments or private actors collect and store vast amounts of personal data without clear safeguards. This raises urgent questions about who has access to the data, the purposes for which it can be used, and the potential for abuse or tampering. The misuse of personal data can lead to harassment, blackmail, or even the suppression of dissent. Furthermore, when private companies or cybercriminals gain unauthorised access to identity databases, individuals are exposed to risks such as identity theft and surveillance capitalism. The right to privacy is a fundamental human right, and any restrictions on it must be lawful, necessary, and proportionate in accordance with international standards.

Closely related is the potential for mass surveillance, especially as digital ID databases are increasingly integrated with biometric technologies and artificial intelligence. In authoritarian or semi-authoritarian contexts, governments may use these systems to track political opponents, suppress activism, or control online behaviour. The military regime in Myanmar, for instance, has used its e-ID system to create a centralised biometric registry of citizens, fueling fears of State overreach and repression. Such indiscriminate and disproportionate data collection, often without individual consent, undermines civil liberties and leads to a chilling effect on freedom of expression and association.

Moreover, accountability and access to remedies remain underdeveloped in many digital identity frameworks. Without clear procedures for correcting errors in biometric or demographic data, individuals, especially those living in poverty, may find themselves unable to access basic public goods such as education, healthcare, or social protection. Legal and institutional mechanisms for grievance redress are often inaccessible or ineffective, leaving affected individuals without a clear path to justice or a remedy.

Lastly, transparency and informed consent are foundational yet frequently neglected principles in the rollout of digital identity systems. Citizens often lack clear, accessible information about what data is being collected, how it will be used, and what rights they have over their personal information. In the absence of strong legal protections, individuals are unable to give free informed consent, leading to erosion of trust and heightened

vulnerability. Rights-respecting digital identity systems must therefore ensure that users are fully informed and empowered, with mechanisms to opt in or out, challenge misuse, and seek recourse when harms occur.

Reflection and Discussion:

Do you know what personal data your government collects on you, and what it is allowed to do with it? Is this information accessible anywhere?

4.2.3 Model Governance Framework for Digital Legal Identity Systems

The UNDP, in collaboration with the Norwegian Ministry of Foreign Affairs, has developed a Model Governance Framework for Digital Legal Identity Systems to guide the development of digital identity systems such that they are rights-based and inclusive. The framework has eight elements: equality and non-discrimination; accountability and the rule of law; legal and regulatory framework; capable institutions; data protection and privacy; user value; procurement & anti-corruption; and participation and access to information. This section discusses some of these elements.

Equality and non-discrimination: A digital identity (ID) system should be designed to protect against discrimination on grounds prohibited under the human rights framework, such as sex, race, ethnicity, religion, and disability. The system should also protect the rights of non-citizens. Furthermore, the system should be designed to allow individuals without proof of legal identity to also verify their identity. To ensure digital identity systems do not violate the right to equality and non-discrimination, the UNDP project suggests that it is essential to consider the following questions:

- Do the Constitution and other laws protect against discrimination?
- Do the substantive laws and procedures for implementing the digital ID system treat women and men equally? If there are differences, for example, if a married woman faces difficulty because she has had to change her name after marriage, this means the digital ID system is not equal for all.
- Are there measures in place to ensure that people are not excluded from registration based on sex or gender identity? Not everyone fits neatly into the male or female category. Digital ID systems must be able to recognise this and also not discriminate against people who do not fit into the male/female category.
- Do the substantive law and procedures for implementation of the digital ID system treat members of different religions, ethnic groups, etc., equally? Digital ID systems should be accessible to all, even if a person lives in a remote location, is not online, or does not have standard identity documents such as birth registration.

Legal and regulatory framework: Under digital ID systems, the State collects and stores personal data of people under its jurisdiction. This raises questions about who may have access to such data, for what purposes it could be used, and whether it can be tampered with. For these reasons, a digital identity system must be established under a law. A legal and regulatory framework is critical, as it ensures that the system‘s management is based on the rule of law and is accountable. This element is interlinked with that of data protection and privacy. The law must establish the elements of the digital identity recorded in the system, including where they are recorded, as well as the authority for the digitalisation of the identity system. The legal framework must have explicit provisions regarding data privacy and protection. Unauthorised use of personal data could lead to violations of the right to privacy, blackmail or suppression of dissenting voices. In addition to the risk that States may use data to consolidate their power, non-state actors may gain access to personal information to market their products or even commit cyber fraud.

As above, to ensure strong legal protection, the UNDP project suggests that it is essential to consider the following questions

- Is there a law backing the digital ID system? Are there clear regulations for implementing the digital ID system?
- Does the law establish the relationship of the digital ID system that is under development with the prior or co-existing (non-digital) registration systems, such as the civil registration system or the voter registration system?

- Does the digital ID system support civil registration? For example, if a person lacks a birth certificate, is there a system in place to ensure that enrollment in the digital ID system also serves as an opportunity for late birth registration?
- Is enrollment in the digital ID system mandatory in law or required in practice for all citizens and /or all residents to access their rights?
- Does the country have a data protection and privacy law in place?
- What is the best practice for data storage and handling? (e.g., centralised, decentralised, federated?) How protected is the user's data? What are the risks if there is a breach?
- Who owns, manages and stores ID? (If the security sector is the leading agency to own, manage and store ID, is there a comprehensive mechanism that limits the usage of the data for specific purposes only?)
- Is there a cybersecurity legislation or regulation?

Accountability and the rule of law: A digital identity system, its management, and impact should be accountable and subject to the rule of law. The system must provide easily accessible mechanisms to address grievances arising from it and offer remedies and redress. For example, a person who wishes to change or correct details registered in the digital ID system must be able to get the details changed within a reasonable time. In the absence of clear mechanisms for providing remedies, it can be challenging to correct errors in biometric recordings. Since digital identity controls access to public goods and services, such as education, healthcare, and social security, people experiencing poverty become disadvantaged on multiple fronts. The questions that should be examined in this regard are:

- Is a person who wishes to change /correct details registered in the digital ID system able to get those details altered within a reasonable time frame?
- If a person is denied enrollment or the ability to correct data, are the reasons for refusal recorded in writing and notified to the applicant? Does the law governing the digital ID system recognise the right to access remedies? What are the available remedies?
- What institutions exist, established by law (constitution or legislation), that have the mandate for independent oversight of executive decisions relating to the digital ID system (e.g., human rights commissions, ombudsperson, data protection commission)? Are these bodies generally regarded as being sufficiently independent and having sufficient powers to exercise their role?

Access to Information: Another important principle is that all information about digital identity systems should be easily accessible to the public. Thus, all residents and citizens should have easily accessible information about: the requirements to register for a digital ID; the services accessible through the digital identity; the rights available to users, such as in the event of misuse of personal data; and the mechanisms available to seek remedy and redress.

Case Study: Aadhaar, India's Extensive Biometric Identification Program

Aadhaar is one of the world's most extensive biometric identification programs, launched in India in 2008 by the Unique Identification Authority of India (UIDAI). It aimed to provide digital identities to 1.2 billion people by 2016, replacing various existing identification forms (e.g., voter ID and ration card, a card for accessing goods under the Public Distribution System) with a single biometric system to make access to public services more efficient. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, provided its legal basis. The constitutionality of the Aadhaar Act was reviewed by the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India (2018). The Court addressed concerns regarding privacy, dignity, and the legality of making Aadhaar mandatory for government subsidies.

Majority Opinion:

Right to Privacy: The Court held that Aadhaar would not constitute a surveillance State, stating that only minimal demographic and biometric data was obtained, and sufficient safeguards, such as encryption and time limits on data storage, were in place. It concluded that the Aadhaar Act did not violate the right to privacy as it passed the threefold test of legality, need, and proportionality.

Right to Dignity: The Court observed that Aadhaar helped disadvantaged sections of society lead a dignified life by ensuring better targeting of subsidies and State benefits, thus facilitating the practical realisation of

various socio-economic rights. It balanced individual dignity with a community approach to dignity, accounting for the "common good" and "public good".

Mandatory for Subsidies: The Court upheld the provision making Aadhaar mandatory for availing State subsidies, benefits, and services. However, it ruled that Aadhaar could not be compulsory for elementary education, as education is an entitlement, not merely a State benefit.

Dissenting Opinion (Concerns):

Privacy and Dignity Violations: The dissenting judge highlighted that biometric data is unique and intimately connected to the individual, making concerns about its security particularly significant. The judge observed that informational privacy is essential for dignity and self-respect, and that once a biometric system is compromised, it is compromised forever. The judge noted that the Aadhaar Act was silent on informed consent and lacked a procedure for individuals to access, correct, or delete their data, thus violating the fundamental principle of personal data ownership and informational privacy. The judge further observed that the "Do No Harm" Principle required the government to maintain continuous oversight and thorough evaluation of the use of biometric and digital identity technologies to ensure they did not cause harm to the individuals concerned.

Exclusion from Benefits: The dissenting opinion found that flaws in the Aadhaar framework and failures in authentication led to the denial of benefits and exclusion of individuals, particularly the marginalised. It stated that an individual's dignity should not depend on algorithms or technological vulnerabilities, and that exclusion due to technological errors violates dignity.

Since the judgment, there have been allegations that the Indian State is using Aadhaar biometric data for surveillance and law enforcement. Practical problems such as bogus and duplicate Aadhaar numbers, inadequate biometric quality, and authentication failures continue to exclude the poor and marginalised from social security support and public services linked to the system. Alarmingly, personal data of 815 million Indian citizens, including Aadhaar numbers and passport details, was reported to have been sold on the dark web in 2023, increasing the potential for cybercrimes and risking information relating to bank accounts and telephone numbers. These issues underscore the ongoing challenges in ensuring the security, privacy, and equitable impact of extensive biometric identification programs.

Reflection and Discussion

The Supreme Court of India upheld the Aadhaar system. However, numerous problems have emerged since its adoption, including citizens' inability to correct their biometric data, failures in biometric authentication, and security concerns about biometrics, among others. Furthermore, because Aadhaar cards are linked to the delivery of public services, the poor and marginalised are often excluded from social security support. There are also reports of the State's use of biometrics for surveillance.

How does the digital identity system of your country compare?. Does it have adequate safeguards to prevent misuse and abuse of biometric information? Does it comply with the Model Governance Framework for Digital Legal Identity Systems developed by the United Nations Development Program?

4.3 Exercising the Rights to Vote and Participation in Public Affairs in the Digital Environment

Emerging technologies are reshaping how individuals participate in governance, access information, express their views, and associate with others. These advancements offer opportunities for empowerment, as much human rights advocacy now occurs online. But they do have challenges, including new forms of manipulation and repression. Rights to information, free speech and expression, and association are deeply interconnected with the rights to vote and participate in governance. Emerging technologies, particularly AI, are influencing the exercise of these rights in both positive and negative ways.

4.3.1 Impact on Electoral Process

Emerging technologies and AI are used in various ways in elections. Political parties may use AI to develop electoral campaigns and influence message development and distribution. While these technologies can make positive contributions to election management, they also present potential for abuse and misuse. Machine learning algorithms can be used by political parties to predict voter behaviour and tailor campaign efforts at the individual level. This is now happening on social media, where people are receiving specific messages based on their demographic identity and may be denied messages from other political parties. Chatbots can engage directly with voters, answer questions, and provide real-time updates. This can be useful when delivering necessary information, but it can also be abused to distribute fake or biased information. AI-generated content can contain inaccuracies or misleading information if not properly overseen.

There are three broad categories of application of emerging technologies in electoral processes: message development and distribution by political parties, organisational management and mobilisation, and election administration (See Table 4.2).

Table 4.2: Application of AI Technologies in Electoral Processes

Domain	Application of AI	Explanation
Message Development and Distribution by Political Parties	AI-driven content creation and targeted messaging	Political parties use machine learning and data analytics to study voter demographics, social media interactions, and behavioural trends. This allows them to craft tailored campaign messages for diverse groups and adjust narratives in response to shifting public sentiments.
Organisational Management and Mobilisation	Internal party strengthening and volunteer engagement	AI tools support parties in analysing which types of content most effectively resonate with members and volunteers. Predictive analytics help optimise resource deployment, improve volunteer training, and enhance mobilisation strategies, making party organisation more efficient.
Election Administration	Enhancing efficiency and accuracy in election management	Election management bodies increasingly rely on AI for maintaining accurate voter registration databases, preventing duplication or fraud, and streamlining election-day operations to ensure smoother and more reliable processes.

Research by the Council of Asian Liberals and Democrats (2024) shows that one risk of using AI is its potential to reinforce existing biases. AI models trained on incomplete datasets can replicate biases, creating content that disproportionately favours particular perspectives or specific voter segments. This contributes to the creation of "filter bubbles" that provide information of a particular nature and limit voters' exposure to other viewpoints. Political parties use this to reinforce existing values and can drive people to become more extreme in their opinions because they do not hear any counter-views. Another risk identified is the potential for misinformation. AI-generated content can include inaccuracies or misleading information. However, AI can also make positive contributions to election management and the electoral process, as illustrated below.

Case Study: Use of Emerging Technologies in the Electoral Process in Indonesia

The 2024 general elections in Indonesia demonstrated the benefits of using AI to facilitate electoral and political processes, as well as the associated risks and challenges that such technologies pose.

The election management body of Indonesia, the General Elections Commission of Indonesia (KPU), has taken measures to integrate emerging technologies into various aspects of election administration. One such measure was the use of the Voter List Information System (Sidalih or Sistem Informasi Data Pemilih), an AI-powered tool launched in 2014, to centralise voter data and identify duplicate entries. Other such systems included the Nomination Information System (Silon) for managing candidate nominations and the Counting Information System (Situng) for facilitating voter tabulation. While the use of such tools increased operational efficiency,

it also posed some challenges. It was reported that 1.9 million Indigenous forest dwellers were omitted from the voter list due to eKTP barriers.

AI tools were also extensively used in election campaigning by all political parties. In the months leading up to Indonesia's general election in February 2024, AI-generated cartoons of presidential candidate Prabowo Subianto were displayed on streets and on social media. The politician, a former special forces general with a documented history of alleged human rights abuses, was portrayed as a grandfather who danced with his cat. This cartoon avatar quickly became popular among his supporters, who branded him as "gemoy", a term used for anything cuddly and lovable. The images were used on street posters, clothing, and other merchandise, while the videos went viral on TikTok. The campaign managers sought to target Indonesia's young, social media-savvy voters who may have been uninformed about his political background.

AI was also used to amplify disinformation. AI tools were used to create fake news and deepfake videos for disseminating false narratives. Some examples included a fake video showing Anies Baswedan, one of the candidates, speaking fluent Arabic. The purpose of such a video could be to manipulate the perception of Muslim voters by building his image as a scholarly Muslim figure. Another example of such disinformation was a documentary on YouTube titled "Dirty Vote", which alleged that outgoing President Joko Widodo secretly channelled State resources to support Prabowo Subianto's campaign. The presidential office denied the claims. Both these videos went viral, attracting millions of views, highlighting the deep penetration of AI-generated misinformation.

Research indicated that the circulation of fake news and hoaxes had drastically increased during the run-up to the 2024 General Elections in Indonesia. Such news was disseminated through various platforms, including YouTube, TikTok, Facebook, Twitter, WhatsApp, Instagram, and others. The Chairman of the Praesidium of the Indonesian Anti-Defamational Society (Mafindo) reportedly stated that as the use of AI becomes easier, the challenges of fact-checking are increasing, as it is more difficult to verify audio news with an AI touch. For this reason, the Chairman suggested that it was essential to provide education to the community so that they do not readily accept all information they receive. He indicated that while short-term fact-checking could address the issue of hoax news, in the long term, there was a need for education to strengthen people's critical thinking skills when receiving information through digital services and to prevent them from being misled by their digital behaviour or algorithms.

Reflection and Discussion:

As seen in the case above, emerging technologies have a mixed impact on elections. Algorithms can be used by political parties to predict voter behaviour and tailor campaign efforts accordingly. Chatbots can be used to engage directly with voters, answer their questions, and provide real-time updates on campaign positions or voting procedures. Misinformation can be used to manipulate voter perceptions and influence their voting choices. But not all the technology is bad. Using this case, think:

- *What are the benefits from the use of AI?*
- *How do the benefits compare with the negative impacts?*
- *Is there any way to better regulate information that both respects freedom of expression and eliminates deepfakes, false information, and algorithmically biased distribution?*

4.3.2 Information Sharing, Free Speech, and Digital Repression

Technology has also transformed the landscape of free speech and expression. Social media platforms have expanded individuals' capacity to express their views and disseminate them to broad audiences, thereby diminishing the traditional monopoly held by legacy media institutions over news production and distribution. Today, any individual with internet access and a presence on platforms such as YouTube, Facebook, TikTok, or X can create and broadcast content globally. These platforms are inherently interactive, allowing users not only to publish content but also to engage directly with creators and fellow consumers through features such as comments and live responses.

The democratisation of information production and distribution has also enabled civic mobilisation and political activism. Around the world, global movements have been initiated through online campaigning, such as the Arab Spring uprisings of 2010-2012, the # MeToo movement, and even the Ice Bucket Challenge. In Southeast Asia, a notable example includes the Bersih movement for electoral reform in Malaysia. However, while social media has been used to mobilise political protests, it also becomes a space where different groups try to suppress the opinions of others, such as the doxing and red tagging campaigns in the Philippines, or the racist targeting of the Rohingya in Myanmar.

States have responded to the potential of the internet by enhancing their capacity to repress it when needed, such as to reinforce political control and ensure their survival. Such measures taken by States can be examined under two broad categories: infrastructural manipulation and informational manipulation. Infrastructural manipulation involves controlling digital infrastructure and the information/communication grid, such as through internet shutdowns. Information manipulation involves deliberately spreading disinformation and bias to influence the information individuals receive.

Governments in Southeast Asia are increasingly deploying advanced surveillance technologies, including social media monitoring, to suppress dissent and control public discourse. Restrictive laws, such as cyber libel regulations, further limit freedom of expression and target critics. Table 4.3 presents examples of digital repression by ASEAN states, adapted from Sriyai's study.

Table 4.3: Type and Measures of Digital Repression by States

Infrastructural Manipulation	Informational Manipulation
• Internet filtering	• Social media monitoring capability
• Internet shutdown	• Domestic dis/misinformation campaigns by the State

Philippines (Domestic Dis/Misinformation Campaigns by the State)

After President Rodrigo Duterte won the 2016 elections, his campaign machinery began targeting news organisations with messages about corruption in the media and attacks on the credibility of journalism and individual journalists. One such target was Rappler, an online news site based in the Philippines and founded by Maria Ressa, which had been publishing stories critical of the government's policies, including reports on the extrajudicial killings associated with Duterte's war on drugs. Pro-government bloggers and automated social media accounts were used for such harassment. Apart from journalists, opposition politicians were also targeted during his presidency. Senator Leila de Lima, a former chair of the Philippines Human Rights Commission and a prominent critic of President Duterte, was targeted with a social media campaign. In February 2017, she was arrested on politically motivated charges. Ressa, herself, was arrested multiple times on charges of cyber libel. A research study examining posts on Facebook and Twitter (now X) found that the attacks against Ressa appeared to be orchestrated by fake and bot accounts. The responses of Facebook and Twitter to removing such accounts were inconsistent and inadequate.

Cambodia (Internet Shutdowns)

A week before the July 2023 elections, Cambodia ordered internet service providers to block access to independent news websites to suppress challenges to the ruling party and tighten media control. In 2021, Cambodia adopted the Sub-decree on the Establishment of the National Internet Gateway (NIG) to manage all internet traffic into and out of Cambodia. The Sub-decree allows the government-appointed NIG operators to block or disconnect any online connection, retain traffic data for a year and provide network information as requested by authorities. The purpose of the NIG, as stated in the sub-decree, is to preserve social order, culture and national tradition. Further, Cambodia's growing dependence on surveillance technology from China raises worries about increased surveillance, censorship, and human rights violations.

Myanmar (Domestic Dis/Misinformation Campaigns by the State)

In August 2017, after coordinated attacks by the Arakan Rohingya Salvation Army, the Myanmar military responded with widespread atrocities against the Rohingya civilian population, including extrajudicial killings and sexual violence. It emerged that the Facebook platform had been used to craft a hate campaign against Rohingya Muslims and spread negative perceptions against them amongst the general public. Such a campaign was constructed by nationalist political parties and politicians, as well as monks, academics, prominent individuals and government officials. Further, since the 2021 military coup in the country, privacy rights have been severely eroded in the country. Laws such as the Cyber Security Law (2025) have been adopted, allowing the junta to access private data under "national security" claims and to retain user data on state-controlled servers.

Vietnam (Internet Filtering, Social Media Monitoring)

Vietnam has been blocking internet content critical of the State and, in 2024, adopted a Decree requiring offshore internet providers to monitor platforms, remove content deemed illegal under Vietnamese law and submit compliance reports. The State has also arrested bloggers, rights campaigners, and activists for voicing opinions on social and political issues via social media.

Singapore (Laws for Repression)

Singapore adopted the Online Criminal Harms Act (OCHA) in 2023 to counter online criminal activity and protect against online harms. This law, having extra-territorial application, grants broad powers to issue directions regarding content restriction, account blocking and app removal to entities facilitating online content. Human rights organisations have raised concerns that such a law can facilitate the arbitrary exercise of power against dissenting voices. Additionally, the Protection from Online Falsehoods and Manipulation Act (POFMA), enacted in 2019, grants the government broad discretionary powers to censor online content and has been used to silence independent media, opposition politicians, and civil society actors.

Reflection and Discussion:

Select a country in Southeast Asia.

- *Check whether there are laws to address cybercrime, computer crime, online falsehoods or other such issues?*
- *What is the stated purpose of these laws?*
- *Analyse how these laws have been applied and implemented. Have they been used for infrastructural and informational manipulation? If yes, in what ways?*

4.3.3 Responsibilities of Big Tech in the Digital Space

While social media platforms offer avenues for individual expression and information sharing, they have also been exploited by States to manipulate data and spread misinformation, serving real political interests. Big Tech, through its actions and inactions, has contributed to these forms of manipulation. Critical questions concerning Big Tech in the context of digital citizenship and citizens' rights to information and free expression include:

- What are Big Tech's responsibilities in addressing fake news and hate speech that provokes conflict and violence between communities?
- What are Big Tech's responsibilities when States request filtering information on social media platforms?
- What are Big Tech's responsibilities concerning the user data gathered by them?

The **United Nations Guiding Principles on Business and Human Rights (UNGPs)** provide guidance on the obligations of Big Tech companies to respect and protect human rights. The UNGPs are structured around three pillars: the State's obligations to protect human rights (Pillar 1); the obligations of businesses to respect human rights (Pillar 2); and the obligation to provide a remedy (Pillar 3).

While States have adopted laws against cybercrime, fake news, and for maintaining public harmony, they have also used these laws to filter internet information, creating dilemmas for Big Tech such as whether they should comply with a government order to restrict content (obligation to follow the laws of a country), or risk their operations in the country by refusing to comply (obligation under Pillar 2, UNGPs). Big Tech companies have attempted to address such dilemmas by adopting transparency measures. For example, when a country requires X (formerly Twitter) to remove content, it often implements the request with "withheld in country" notices, making the content visible globally but inaccessible within the requesting country. X also publishes transparency reports detailing government requests for content removal and account information, which are crucial for public accountability. Similarly, Meta has developed "community standards" for content moderation across its platforms (Facebook, Instagram, Messenger, Threads), focusing on issues such as violence, harassment, and hateful conduct. Meta has also established an Oversight Board to provide policy recommendations and serve as an independent check on its content moderation practices in line with community standards. While these standards are promising starts, they should be put into context with the amount of hate speech, gender-based hate speech, bullying, racial vilification, and disinformation distributed by these networks. While the platforms may claim that these negative aspects are permitted under freedom of expression, there is little respect for users' rights (Pillar two of the UNGPs) and few avenues for people whose rights have been violated to find justice (Pillar three).

Another concern is corporate surveillance. Corporate surveillance is primarily driven by the profit motives of Big Tech like Google, Meta, Amazon, and TikTok, aiming to refine products, deliver targeted advertising, and enhance user services. These companies engage in pervasive data collection, systematically extracting information through tools such as browser cookies, web beacons, mobile apps, and third-party scripts that track users across digital spaces. This data, including browsing history, clicks, location, and search queries, is analysed using algorithms and machine learning to create highly detailed user profiles for content personalisation and revenue generation. Through data aggregation, data from different platforms and IoT devices, such as smart thermostats and fitness trackers, are merged to develop predictive consumer models that can be sold or used internally. Corporations can use such personal data for purposes such as political profiling, targeted advertising, behavioural nudging, or influencing voting patterns, as evidenced by the Cambridge Analytica scandal.

The use of data by Big Tech in these ways raises human rights concerns about privacy due to unclear data practices. Users are often unaware of what data is collected, processed, or shared. Consent mechanisms are frequently buried in lengthy privacy policies, undermining meaningful user control. Further, the concentration of power held by these tech giants also raises questions about democracy and public accountability, as their business priorities may not always align with democratic values, potentially exacerbating State efforts to suppress dissent.

You Are Here: You Are More Predictable Than You Think

Digital systems are designed to anticipate what you might buy, believe, or click next. Over time, these predictions can influence your choices, nudging behaviour while giving the illusion of freedom.

4.4 Use of Emerging Technologies by Courts and Law Enforcement

Another essential aspect of citizenship is the right to equal protection under the law. Judiciaries and law enforcement agencies across Southeast Asia are progressively adopting emerging technologies such as artificial intelligence (AI), facial recognition systems, predictive analytics, and blockchain applications to enhance the efficiency of the judicial and law enforcement systems. Since August 2023, the Singapore Judiciary, in collaboration with a private company, has been exploring the use of generative AI technology to support cases under the Small Claims Tribunals (SCT). In the first step, an on-demand translation service was introduced, allowing court users to obtain generative AI-powered translations of court documents into Chinese, Malay, and Tamil. Subsequently, generative AI tools have been developed that can summarise case documents for the Tribunal magistrates and individuals representing themselves in the SCT. In Malaysia, the Artificial Intelligence in Court System (AiCOS) is a pilot project in Sabah and Sarawak to assist judges in achieving

greater consistency in court sentencing for offences related to drug possession and rape. In Indonesia, AI is being applied by law enforcement for detecting financial crimes, facial recognition for suspect identification, and data analysis for crime prediction, among other applications.

While the use of AI has its advantages, such as enhancing procedural efficiency, there are also concerns that tools like facial recognition or police drones may be misused. Use of AI in judicial sentencing raises fears that reliance on generative AI may not only amplify biases against minorities and marginalised groups, but may also lead judges to overlook mitigating factors and circumstances while sentencing, leading to the awarding of unfair punishments.

UNESCO has developed "Draft Guidelines for the Use of AI Systems in Courts and Tribunals", published in 2025. These guidelines prescribe fifteen principles for the development, acquisition, adoption, deployment and use of AI systems by the judiciary. A summary of the principles is in Table 4.4 below:

Table 4.4: Draft Guidelines for the Use of AI Systems in Courts and Tribunals (UNESCO), 2025 Summary

Protection of human rights	Necessary steps should be taken to respect, protect and promote human rights and the rule of law. Specifically measures should be taken to: • Prevent biased development and applications of AI systems and outcomes that may aggravate, reproduce, reinforce or perpetuate discrimination in society. • Ensure equal access and treatment for all before the courts regardless of their digital capacity. • Assess the implications of AI systems for procedural fairness and prevent applications that violate the rights to fair trial. • Protect privacy and personal data. • Ensure that individuals are not detained based on decisions assisted by AI that the individual is not aware or, or is unable to understand how the AI system reached the decision. Furthermore, the individual must be able to file appeal the decision making process and the decision itself.
Proportionality	The AI system used must meet the requirements of legitimacy and proportionality. In cases where the impact of decisions made by AI is difficult to reverse or irreversible (involving life-or-death decisions), final determinations should be left to humans.
Information security	AI systems should protect confidential information in line with international standards and establish safeguards against cyber threats.
Explainability	AI systems should be able to explain the rationale behind their outputs and the inputs used to generate them.
Transparent and open justice	There should be transparency regarding how the AI system was developed, how it operates, its training data, and its limitations.
Awareness and informed use	The AI system should have been adopted after informed discussion on its functionalities, types of uses, potential impacts, limitations and associated risks.
Accountability and contestability	There should be mechanisms that allow affected parties to contest and cross-examine any output produced by AI systems, as well as to hold judicial officers accountable for any errors.
Human oversight and decision making	Judicial offers should not delegate any part of their mandate or rely exclusively on AI systems to make decisions or automate entire processes that may negatively impact the rights of individuals or communities.
Human centric and participatory design	The development and use of AI systems should complement and augment the judiciary's capacities and respect human dignity and autonomy.
Multi-stakeholder governance and collaboration	Judicial stakeholders should consult diverse stakeholders, hold public consultations and implement citizen participation approaches throughout the AI system's life cycle.

Reflection and Discussion:

- *What problems are these principles in the Draft Guidelines of the Use of AI in Courts and Tribunals addressing?*
- *Select a principle and detail the concern or bias they are trying to avoid.*
- *Do the benefits outweigh the concerns?*
- *Should Courts be encouraged to use AI?*

4.5 Surveillance and the Limits of Digital Citizenship

Having explored how individuals participate as digital citizens and exercise their rights within online spaces, it is also important to recognise that these interactions do not occur in a neutral environment. The same technologies that empower users to connect, express themselves, and access information also generate vast amounts of data that can be observed, collected, and analysed by various actors. This brings us to the issue of surveillance, a central feature of the digital ecosystem that shapes how rights are protected, or undermined, in practice. Understanding surveillance is essential because it directly affects the autonomy, privacy, and security of digital citizens.

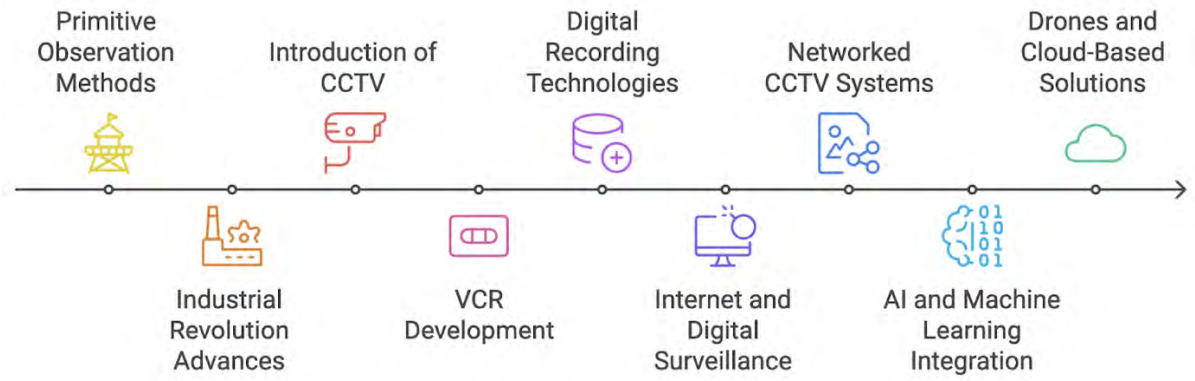
You Are Here: Being Watched Changes How You Behave

Knowing that posts can be tracked, screens captured, or messages monitored often leads people to stay quiet, avoid topics, or censor themselves. Surveillance does not only collect information, it quietly shapes what people dare to say or do.

Surveillance technologies have undergone a remarkable evolution, transitioning from basic observation methods to highly sophisticated systems integrated with artificial intelligence (AI) and cloud computing. Early forms of surveillance in ancient civilisations involved rudimentary techniques like watchtowers and guards. By the late 19th and early 20th centuries, photographic documentation and telephone wiretapping emerged. A significant turning point occurred in the mid-20th century with the introduction of Closed-Circuit Television (CCTV) in the 1940s, initially for industrial use and later adapted for public settings in the 1960s, and with Video Cassette Recorders (VCRs) enabling the storage of footage in the 1970s.

The digital revolution of the 1990s marked a new era, allowing the capture and analysis of massive volumes of personal data through the internet and computer technologies, including email and browser history tracking. The late 20th and early 21st centuries saw further advancements in digital cameras and IP technology, improving image quality and enabling remote access to video feeds. The integration of intelligent video analytics allowed systems to detect trends, recognise faces, and predict security threats. More recently, surveillance technologies have incorporated AI and machine learning, enabling systems to understand what they monitor, detect suspicious behaviour in real-time with unparalleled accuracy, and utilise deep learning for efficient image, facial, and vehicle recognition. Cloud-based solutions have further enhanced accessibility and scalability, while Unmanned Aerial Vehicles (UAVs) or drones now provide aerial reconnaissance capabilities previously impossible, fundamentally transforming surveillance operations. This ongoing progression, integrating AI, big data, and biometrics, underscores the continuous ethical dilemmas and the critical need for holistic legal frameworks to balance privacy and civil liberties.

Figure 4.1: Evolution of Surveillance Technology



Surveillance is conducted using a wide range of technologies. Figure 4.1 describes different types of surveillance technologies. These technologies seem harmless at the outset. For example, nowadays CCTV cameras are common in public places, and their presence is seen as a tool that supports public safety and security. However, such cameras can also be used by the State as tools of surveillance. Table 4.5 illustrates specific types of surveillance technologies and their associated human rights risks.

Table 4.5: Consequences of surveillance technologies for human rights

Type of Surveillance Technology	Description	Common Uses	Human Rights Concerns
CCTV Cameras	Video recording devices that monitor specific areas.	Public spaces, businesses, and residential areas for crime prevention.	May infringe on the right to privacy, especially in public or personal spaces.
Facial Recognition	AI technology that identifies individuals by their facial features.	Airports, law enforcement, and event security.	Risks wrongful identification and can target specific groups, impacting equality and freedom from discrimination. Some faces are easier to recognize than others.
GPS Tracking	Uses satellite signals to track location in real-time.	Vehicle tracking, delivery services, and personal mobile devices.	Continuous location tracking may violate personal privacy.
Social Media Monitoring	Analyzes user activity on social media platforms.	Used by businesses for marketing and by governments for security.	Infringes on freedom of expression, as individuals may self-censor knowing they are being monitored. Does not respect private communications
Biometric Scanners	Devices that scan fingerprints, iris, or voice for identification.	Secure facilities, banking, and smartphones.	Collection of sensitive data can lead to misuse, impacting the right to privacy and data protection.

Type of Surveillance Technology	Description	Common Uses	Human Rights Concerns
Drones	Unmanned aerial vehicles used for remote surveillance.	Border control, disaster response, and crowd monitoring.	Can infringe on privacy rights when used over private areas without consent.
AI and Predictive Analytics	Analyzes large data sets to predict behaviors or security threats.	Law enforcement and corporate security.	May result in profiling and bias, affecting rights to equality and fair treatment.
Internet Data Collection	Collects and analyzes data from browsing history and online activities.	Marketers and government agencies for tracking.	Can lead to misuse of personal information, violating privacy and personal data rights.

Surveillance is conducted at various levels by different actors, each with distinct purposes and significant impacts on individual privacy and societal dynamics.

4.5.1 Surveillance by State

Governments claim to employ surveillance to safeguard national security, uphold law enforcement, and maintain public order. This increasingly relies on advanced technologies for the systematic monitoring of both large populations and specific individuals. While this does occur, there are numerous cases where this power has been abused. Mass surveillance methods, such as the indiscriminate collection of internet data, telecommunications metadata, and real-time video feeds, pose serious challenges to privacy and civil liberties. While often rationalised for counter-terrorism purposes, mass surveillance remains contentious in democratic countries as it threatens civil liberties. Targeted surveillance, focusing on specific individuals or groups deemed threats, also frequently breaches ethical boundaries by infringing on privacy and freedom of expression. Biased algorithms in facial recognition technology can lead to incorrect identifications, police harassment, and systemic discrimination.

Most States have enacted laws on cybercrime, telecommunications, electronic transactions, public safety, etc., that give authorities the power to intercept communications, monitor online activity, and preserve computer data and traffic. In the absence of adequate legal and judicial safeguards, States can use such laws to monitor the activities of opposition groups, dissidents, human rights activists, and journalists. Further, in the absence of adequate data protection laws, private entities can also use user data for various purposes without seeking user consent. The case studies from different countries highlight the different forms of surveillance in the region.

Case Study: Pegasus Spyware Targeting Activists

Thailand has faced serious concerns regarding government surveillance, notably the deployment of Pegasus spyware to target political opponents, activists, and academics. This Israeli-made spyware can infiltrate mobile devices without the user's knowledge, accessing personal data and communications. A joint investigation revealed that individuals were infected during a surge in pro-democracy activism. Critics argue this violates privacy rights and freedom of expression, constituting an abuse of power to silence dissenting voices. The psychological impact has created a climate of fear, undermining democratic freedoms.

Case Study: MySejahtera App – From Public Health to Public Outcry

The Malaysian MySejahtera app, initially for COVID-19 contact tracing, raises surveillance and human rights concerns in Malaysia. Despite government assurances of data protection, an Auditor-General's report revealed potential data leaks, including a "super admin" account downloading millions of information sets and the app being subjected to numerous attacks. Uncertainty over the app's ownership, linked to a private company reportedly controlled by political associates, further fueled concerns about data privacy and potential misuse of extensive personal information, including location and health data, collected from over 38 million users. Critics argue that the app's lack of transparency and Malaysia's weak privacy laws expose citizens to privacy breaches, highlighting the delicate balance between public health measures and individual privacy rights.

Case Study: "Lamppost-as-a-Platform" initiative

Singapore's "Smart Nation" initiative incorporates advanced surveillance to enhance urban management, traffic flow, and public security. Investments include a network of 110,000 lampposts equipped with sensors and surveillance cameras featuring facial recognition technology. While aiming to enhance urban security, this raises the risk of mass surveillance, where individuals are constantly monitored without their knowledge or consent, undermining the fundamental right to privacy. The "Lamppost-as-a-Platform" initiative explicitly seeks to introduce facial recognition technology in public areas, sparking discussions about widespread surveillance. Critics contend that the perception of continuous surveillance can lead to self-censorship, limiting freedom of expression, public debate, and democratic participation.

Case Study: SIM Cards with Multiple Functions

In Laos, the government has mandated SIM card registration for all citizens, aiming to eliminate online anonymity and enhance State control over telecommunications. Users are required to use a specific app that requests access to personal data such as contacts, GPS location, and device storage. While justified as a measure to combat criminal activities like fraud and online scams, critics argue this initiative has dual goals: crime prevention and increased surveillance and control over the population. In a country where dissent is frequently suppressed, the potential misuse of collected data poses a significant threat to individual freedoms.

Case Study: Indonesia

Indonesia's 1945 Constitution (Article 28G) protects personal privacy and the secrecy of communications. Yet, this right has been significantly weakened by two major laws: the Electronic Information and Transactions (EIT) Law of 2008 (amended 2016 and 2024) and the Cybersecurity Law of 2019 (strengthened 2022–2024). These laws grant police, intelligence agencies, and the national cybersecurity body broad authority to monitor, in real time, intercept messages, access private data from internet companies, and monitor electronic communications with minimal judicial oversight, few clear limits, and no independent approval required in most cases. Intended initially to support e-commerce and defend against cyber threats, the laws have instead enabled widespread surveillance of activists, journalists, students, religious minorities, and Papuan independence supporters, creating a chilling effect on free expression, assembly, and association. Although Indonesia passed a Personal Data Protection Law in 2022, its many national-security exceptions and the still-weak oversight body leave constitutional privacy promises largely unfulfilled, illustrating a common pattern in emerging democracies. Strong rights that look strong on paper are quietly undermined by vague, security-focused legislation and advancing surveillance technology.

At the international level, global surveillance networks expand the scope of monitoring, with collaborations such as the Five Eyes Alliance (comprising the US, UK, Canada, Australia, and New Zealand) enabling intelligence sharing among countries. While these networks aim to enhance global security, they often operate with minimal transparency, raising questions about accountability and sovereignty as well as the extraterritorial application of human rights treaties to foreign surveillance activities.

4.5.2 Workplace Surveillance

Employers monitor employees to enhance productivity, ensure security, and protect company assets. This can range from tracking digital communications (emails, browsing history, keystrokes) and physical movements (GPS tracking, CCTV) to using AI tools to gauge employee sentiments. While workplace surveillance can improve efficiency and prevent misconduct, it raises significant concerns about privacy, consent, and the potential for abuse, often breeding mistrust and hindering creativity. Despite privacy rights being enshrined in global human rights agreements, employees may not fully understand the scope of surveillance, affecting their capacity to provide effective consent.

Marginalised groups, particularly lower-income workers or those in precarious employment, are especially vulnerable to exploitation through invasive monitoring. For example, workers in the gig economy (e.g., food delivery, ride-hailing services like Gojek, Grab, or Foodpanda) are constantly monitored via GPS tracking and mobile apps that record location, delivery times, and response speed. This continuous monitoring can lead to fewer jobs or suspension for minor deviations, forcing workers in unstable employment to accept intrusive surveillance without question or recourse. In many Southeast Asian countries, existing legal frameworks often lag behind technological advancements, creating loopholes that allow employers to engage in invasive monitoring practices without adequate oversight. Singapore's Personal Data Protection Act (PDPA), for instance, contains broad exceptions that permit employers to monitor employees under the guise of protecting business interests.

4.5.3 Individual and Peer-to-Peer Surveillance

Surveillance is no longer exclusive to institutions; individuals now monitor others using accessible technologies, often informally. Parental monitoring of children's online activities, social interactions, or whereabouts using parental control apps or GPS tracking, while aiming to enhance safety, can impede children's independence and infringe on their privacy. Monitoring by spouses or partners through tracking apps or spyware programs can escalate to abusive behaviour, raising serious protection concerns for women who may be escaping an abusive relationship. Community surveillance, facilitated by tools such as neighbourhood watch apps and home security systems, can deter crime but may also lead to increased over-policing or intrusions into neighbours' privacy.

Reflection and Discussion

- *When, if ever, should national security justify secret mass surveillance without a judge's warrant?*
- *Why is the argument "I have nothing to hide" insufficient in a democracy?*
- *What three concrete safeguards would you add to Indonesia's surveillance laws to better protect human rights while still addressing real security threats?*
- Do global technology companies have a responsibility to resist government surveillance demands, even if it risks being banned in that country?

4.6 Conclusion

We are living through the largest identity experiment in history. Billions of people now have a permanent digital shadow that follows them from school to job interviews, from borders to hospital beds, from the moment they wake up to the moment they sleep. In Southeast Asia this shadow is growing fastest: national digital IDs, COVID-tracing apps that never went away, private companies scoring "trustworthiness," and cameras that recognise faces in real time. The promise was inclusion, bank accounts for the unbanked, faster government services, and safer cities. The reality is often control: minorities profiled, activists silenced, ordinary people afraid to speak or gather. When every action leaves a trace and every trace can be punished, freedom itself is at risk. Yet resistance is also digital. Young people are choosing encrypted messengers, demanding data rights, building alternative platforms, and refusing to accept that convenience must come at the cost of dignity. The struggle over digital citizenship is not a technical debate—it is the central human rights battle of our generation.

Key Takeaways

1. Digital citizenship refers to the exercise of citizenship rights in a digital environment.
2. Digital identity systems can expand access to services but easily become tools of surveillance and exclusion.
3. Mass data fusion (combining government, telecom, banking, and social-media records) creates detailed profiles most citizens never see.
4. Surveillance produces chilling effects: people self-censor, avoid protests, or change behaviour out of fear.
5. Marginalised groups (ethnic minorities, migrants, LGBTQ+ communities) are hit hardest by identity scoring and profiling.
6. Reclaiming digital citizenship requires strong data-protection laws, decentralised alternatives, and active civic pushback.

Issues to Think About

1. When you scan your national digital ID or health app, do you feel more included or more watched?
2. If a private company gave you a "trust score" that affected your ability to rent a flat or get a loan, would you accept it?
3. Have you ever stopped yourself from posting something online because you worried who might see it later?
4. Should citizens have the legal right to see and correct their complete digital profile held by the government?
5. Which is more dangerous in your country right now: too much surveillance or too little digital inclusion?
6. Imagine a future with perfect digital identity: what is the best possible version, and what is the nightmare version? How do we choose the first and avoid the second?

Further Readings

Digital Identity Systems

UNDP. (2023). *UNDP Model Governance Framework for Digital Legal Identity System*. UNDP Digital Legal ID Governance. https://www.governance4id.org/#Explore

World Bank. (2019). *ID4D Practitioner's Guide*. Identification for Development, World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide

World Bank. (2024). *Identification for Development (ID4D) and Digitalising G2P Payments (G2Px) 2023 Annual Report*. World Bank Group. *https://id4d.worldbank.org/annual-report*

Privacy International. (2020). A Guide to Litigating Identity Systems. In Privacy International. https://privacyinternational.org/sites/default/files/2020-09/PI_A%20Guide%20to%20Litigating%20Identity%20Systems_Full%20version_0.pdf

Aadhar System in India

Ahmed, N. (2023, November 7). How the personal data of 815 million Indians got breached | explained. *The Hindu*. https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece

Banerjee, S. (2015). Aadhaar: Digital Inclusion and Public Services in India, Background Paper. In *the World Development Report 2016, Digital Dividends*. World Bank.

Yadav, A. (2024, December 22). Digital exclusion: The poor elderly face the brunt of Aadhaar-based authentication errors. *The Wire*. https://thewire.in/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors

Panigrahi, S. (2022). Marginalised Aadhaar: India's Aadhaar biometric ID and mass surveillance. *IX Interactions*, *XXIX.2*.

Khera, R. (2019, April 6). Aadhaar Failures: A Tragedy of Errors. *EPW Engage*, *Volume 54, Issue No. 14*.

Misinformation, hate speech, fake news

Freedom House. (2024). Freedom on the Net 2024: The Struggle for Trust online. In *Freedom on the Net 2024*. https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

Amnesty International. (2022). The Social Atrocity - Meta and the Right to Remedy for the Rohingya. In *Amnesty.org* (ASA 16/5933/2022). https://www.amnesty.org/en/documents/asa16/5933/2022/en/

Council of Asian Liberals and Democrats. (2024). AI in elections in East and Southeast Asia: opportunities, challenges, and ways forward for Democrats and liberals. In *cald.org*. https://www.freiheit.org/southeast-and-east-asia/ai-elections-east-and-southeast-asia

Civicus & FORUM-ASIA. (2023, July 11). *Singapore: Online Criminal Harms Act, another legal instrument to suppress civic space* [Press release]. https://www.civicus.org/index.php/media-resources/media-releases/6474-singapore-online-criminal-harms-act-another-legal-instrument-to-suppress-civic-space

Sastramidjaja, Y., & Wijayanto. (2022). *Cyber troops, online manipulation of public opinion and Co-Optation of Indonesia's cybersphere* (Issue 7). ISEAS Yusof Ishak Institute. https://www.iseas.edu.sg/wp-content/uploads/2022/03/TRS7_22.pdf

Fajriansyah, A. (2024, May 2). The spread of hoax news increases during the 2024 election. *Kompas*. https://www.kompas.id/artikel/en-penyebaran-berita-hoaks-meningkat-selama-masa-pemilu-2024

Sriyai, S. (2024). How means for digital repression in Southeast Asia have unfolded in recent times. *Perspective*, *2024*(65). https://www.iseas.edu.sg/wp-content/uploads/2024/08/ISEAS_Perspective_2024_65.pdf

Tulshyan, T. (2024, November 8). *The dark side of generative AI in Prabowo Subianto's presidential campaign*. Columbia Political Review. https://www.cpreview.org/articles/2024/11/the-dark-side-of-generative-ai-in-prabowo-subiantos-presidential-campaign

Rosenkrantz, S. (2022, March 8). *Facebook and Genocide: How Facebook contributed to genocide in Myanmar and why it will not be held accountable - Harvard Law School | Systemic Justice Project*. Harvard Law School | Systemic Justice Project. https://systemicjustice.org/article/facebook-and-genocide-how-facebook-contributed-to-genocide-in-myanmar-and-why-it-will-not-be-held-accountable/#facebooks-role

Ressa, M. & National Democratic Institute. (2018). FORUM Q&A: MARIA RESSA ON DIGITAL DISINFORMATION AND PHILIPPINE DEMOCRACY IN THE BALANCE (D. Jackson, International Forum for Democratic Studies, & National Endowment for Democracy, Interviewers). In the *International Forum for Democratic Studies*. https://www.ned.org/wp-content/uploads/2018/02/Maria-Ressa-on-Digital-Disinformation-and-Philippine-Democracy-in-the-Balance.pdf

Renaldi, A. (2021, April 29). Indonesia's invisible people face discrimination, and sometimes death, by database. *Rest of World*. https://restofworld.org/2021/indonesias-invisible-people-face-discrimination-and-sometimes-death-by-database/

Ressa, M., ICFJ, University of Sheffield, Rappler, Shabbir, N., Aboulez, N., Greenwood, M., Roberts, I., Gorrell, G., Graphika, Heloise Hakimi le Grand, Sharon Moshavi, & Bob Tinsley. (2021). Online violence against Women: A case study of attacks against Maria Ressa. In *ICFJ*. ICFJ, Washington, D.C. https://www.icfj.org/sites/default/files/2021-03/Maria%20Ressa-%20Fighting%20an%20Onslaught%20of%20Online%20Violence_0.pdf

United Nations Human Rights Council. (2018). Report of the detailed findings of the independent International Fact-Finding Mission on Myanmar. In *United Nations* (A/HRC/39/CRP.2). Human Rights Council.

Hassenstab, N. (2024, March 6). *Four questions about Indonesia's presidential election*. American University, Washington, DC. https://www.american.edu/sis/news/20240306-four-questions-about-indonesias-presidential-election.cfm

Hoang, L. (2023, August 16). Vietnam's plan to block users puts internet access at risk. *Nikkei Asia*. https://asia.nikkei.com/Business/Technology/Vietnam-s-plan-to-block-users-puts-internet-access-at-risk

Howard, P. N., & Hussain, M. M. (2013). Digital media and the Arab Spring. In *Oxford University Press eBooks* (pp. 17–34). https://doi.org/10.1093/acprof:oso/9780199936953.003.0001

Human Rights Watch. (2024a, January 11). *Singapore, Events in 2023* [Press release]. https://www.hrw.org/world-report/2024/country-chapters/singapore

Human Rights Watch. (2024b, March 5). *Vietnam:* New Wave of Arrests of Critics [Press Release]. https://www.hrw.org/news/2024/03/05/vietnam-new-wave-arrests-critics

International Commission of Jurists. (2021, May 17). *Indonesia: trans women face discrimination in access to COVID-19 vaccines* [Press release]. https://www.icj.org/indonesia-trans-women-face-discrimination-in-access-to-covid-19-vaccines/

Use of technology in administration of justice

Yanwiyatono, Y., & Nurdin, B. (2024). *Utilisation of Artificial Intelligence Technology in Law Enforcement in Indonesia* (ICLSSEE 2024). EAI. https://doi.org/10.4108/eai.25-5-2024.2349154

Yihan, G. (2024, April 20). "*Perspectives on Artificial Intelligence – A View from Singapore."* The Standing International Forum of Commercial Courts. https://www.judiciary.gov.sg/news-and-resources/news/news-details/justice-goh-yi-han--address-at-the-standing-international-forum-of-commercial-courts

Judiciary Times. (2025, May 1). https://www.judiciary.gov.sg/docs/default-source/publication-docs/judiciary-times-issue-1-2025.pdf?sfvrsn=58d278c1_1

Chapter 5:

Labour and Human Rights in the Automated Age

Reader's Guide

Artificial Intelligence will reshape labour. Whether it is a transformation that creates unprecedented productivity, or job losses, or fundamentally changes the nature of fair work is still open for debate. This chapter starts by examining the differences between automation and AI, and then addresses their impact on the workforce, from the rise of technology-based jobs to the precariousness of the gig economy, where workers often lack social security and collective bargaining power. The human rights implications in the digital workplace are discussed, including the need for states and corporations to uphold human dignity.

In this chapter, you will:

- Understand technology's transformation of labour.
- Explore human rights implications in the digital workplace.
- Understand obligations of state and non-state actors in the business and human rights context.
- Analyse real-world case studies.

This chapter will equip you to understand and advocate for a human-centred approach to labour, ensuring that technological progress creates a future of shared prosperity and justice, rather than one of exploitation and inequality.

Key Terms

- **Automation**: The use of machines or software to perform tasks traditionally done by humans, often rule-based and repetitive, aiming for increased efficiency, productivity, and safety.
- **Technological Unemployment**: The phenomenon of job losses resulting from the replacement of human workers by intelligent systems and AI-driven automation.
- **Platform Economy**: New work models where services are delivered through digital platforms, categorized into location-based (e.g., ride-sharing) and online platforms (e.g., freelancing, food delivery).
- **Social Security Protection**: A human right ensuring individuals can access benefits when they lose work income due to various circumstances (e.g., sickness, unemployment, old age), providing protection from unaffordable healthcare costs.
- **Wage Compression**: An economic phenomenon where wages for low-skilled workers stagnate or decline relative to those of high-skilled workers, often attributed to automation and technological advancements

5.1 The Technological Reshaping of Labour

The advancement of technology has transformed the landscape of human labour. Innovations in artificial intelligence and automation have enhanced productivity and created pathways for inclusivity, potentially empowering vulnerable groups, fostering resilience, improving access to justice, and offering avenues to reduce poverty and advance human rights. However, this technological revolution raises human rights concerns, including equitable access, the risk of job displacement, and fair working conditions.

5.1.1 Automation vs. Artificial Intelligence

While often used interchangeably, automation and artificial intelligence (AI) have different implications for labour. Automation involves using machines or software to perform tasks that would otherwise require human intervention. Historically, automation has been rule-based and predictable, as seen in factory robots assembling components identically every time. These technologies replace routine and repetitive tasks, offering benefits such as reduced unplanned downtime, increased productivity, improved product quality, and enhanced worker safety. This transformation is particularly evident in the manufacturing sector, especially in automotive factories where complex assembly processes are now predominantly performed by precision-engineered machines. However, while these technologies replaced routine tasks and improved safety, they faced limitations in adaptability. The mining industry illustrates the evolution of these systems. While tunnel-drilling machines represent high-precision automation, autonomous haulage systems (self-driving trucks) represent a shift towards AI, capable of navigating complex environments. These innovations enhance operational efficiency and can eliminate dangerous and exploitative work environments, though they still require human oversight - shifting the worker's role from manual operation to system supervision.

Artificial Intelligence (AI), on the other hand, focuses on giving machines the ability to "think" in specific ways, enabling them to learn from data, recognise patterns, and make decisions in unpredictable scenarios. Unlike automation, which executes instructions, AI can analyse, adapt, and improve the process itself. This makes these machines appear more human-like. This capability transforms automation into a more powerful and flexible tool, allowing systems to manage complex, variable situations rather than being restricted to repetitive, routine tasks. AI-driven robotics can address labour shortages, establish safer work environments, and optimise resource use.

Table 5.1 summarises the main differences between automation and AI and their impacts on work:

Table 5.1: Differences between automation and artificial intelligence

Aspect	Automation	Artificial Intelligence (AI)
Core ability	Follows fixed, pre-programmed rules	Learns from data, adapts, and makes decisions
Type of tasks	Repetitive, predictable, rule-based (e.g., welding the same car part every time)	Variable, complex, or creative (e.g., diagnosing diseases from medical images or translating languages in real time)
Flexibility	Low – breaks down if conditions change	High – handles new situations and improves over time
Examples in Southeast Asia	Factory robots in Vietnam's electronics plants; automated packaging lines in Indonesian food factories	AI chatbots used by Grab and Gojek for customer service; AI tools that predict traffic and optimise delivery routes
Impact on jobs	Mainly replaces routine manual or clerical jobs; reduces injuries in dangerous work	Can replace or augment a wider range of jobs; creates demand for new skills (e.g., AI trainers, data analysts) while displacing others
Limitations	Needs human oversight for anything unexpected	Can make mistakes if trained on biased or incomplete data; requires large amounts of data and energy

The key difference lies in their capacity for learning and adaptation: automation executes predefined rules efficiently, whereas AI enables systems to learn, adapt, and make informed decisions, thereby expanding the scope of automated tasks.

5.1.2 AI-Driven Job Replacement and New Work Models

The integration of AI and automation will have significant impacts on the workforce, leading to job replacement and new work models. As AI-driven automation advances, many jobs characterised by repetition, precision requirements, and high-risk environments are being replaced by intelligent systems. This phenomenon has intensified discussions around "technological unemployment," raising concerns about the potential for massive job losses as robots make human workers redundant. The International Monetary Fund (IMF) has warned that AI could affect jobs worldwide, potentially exacerbating inequality if left unchecked.

In Southeast Asia, vulnerability varies by country and sector. Countries such as Indonesia, Vietnam, Thailand, and the Philippines face higher exposure to disruption in routine tasks, whereas Singapore's advanced infrastructure and skilled workforce offer greater resilience. Specific examples illustrate these trends:

- The 2022 Gojek–Tokopedia merger resulted in approximately 1,300 job cuts (12% of the combined workforce).
- The 2022 launch of ChatGPT accelerated disruptions for editors, copywriters, and content creators.
- DBS Bank announced in 2025 plans to reduce around 4,000 temporary and contract positions across 19 markets over three years due to AI adoption, while simultaneously creating approximately 1,000 new AI-related roles, demonstrating a pattern of displacement accompanied by targeted job creation.

These developments underscore fundamental transformations in labour markets, where intelligent systems are displacing traditional, labour-intensive positions across diverse industries and skill levels. Furthermore, AI's influence can lead to wage compression for low-skilled workers, as automation and technological advancements have been linked to significant wage decreases in specific sectors since 1980. The result is that low-skilled workers face lower wages, while professional positions may see increases in compensation, creating greater wage inequality across the workforce.

Despite the challenges of job displacement, this technological revolution also generates novel employment opportunities, particularly the emergence of high-skilled technological roles within information and communication technology domains. These roles, often referred to as "digital jobs," encompass a wide variety of positions across sectors that rely on digital skills and digital technologies. Some companies offer flexible work arrangements, new income-generating opportunities, and remote work, enabling workers to perform tasks from anywhere.

The platform economy is a prominent example of these new work models, with the International Labour Organisation (ILO) identifying two primary platform types:

- Location-based platforms that provide services at specific physical locations (e.g., ride-sharing).
- Online platforms, where services are delivered remotely through digital channels (e.g., freelancing, food delivery).

The ILO, the international organisation with the mandate to ensure workers' standards at the global level, is currently drafting a Convention and a Recommendation on the protection of workers' rights in the platform economy. The governing body of the ILO decided to act on this, given the concerns raised by trade unions and government officials about gaps in protection for platform workers. They have been concerned by the significant challenges for platform workers, such as:

- They often operate outside traditional employment protections, experiencing uncertain employment status and limited job security.
- They face reduced social protection, with typically self-employed classifications often excluding them from employee-based benefits and placing the full contribution burden on individual workers.
- Irregular work patterns, diverse income streams, and the absence of employer contributions create significant barriers to meeting eligibility thresholds and to accessing adequate social security coverage.

- The online nature of platform work also results in a lack of collective worker organisations, leaving these workers particularly vulnerable and without traditional forms of workplace representation and advocacy.
- Micro, Small, and Medium Enterprises (MSMEs) are particularly vulnerable, with many digital platforms operating in regulatory grey areas that minimise worker protections.

These issues highlight the need for rights-based approaches that balance economic growth and technological innovation with social protection mechanisms that ensure fair employment conditions.

Developments in automation, artificial intelligence, and digital platform economies represent a part of the transformations that continue to reshape labour conditions worldwide. While the discussion above highlights important trends, it is not exhaustive, as technological innovation is dynamic. Each new wave of development, whether in robotics, data-driven platforms, AI or emerging forms of digital labour, has the potential to alter how work is organised, valued, and experienced. Future innovations may dramatically redefine both productivity and human work.

The question of whether technology is replacing human workers does not have a straightforward answer. Much depends on how societies choose to design, deploy, and regulate new technologies. Despite the rapid spread of digitisation and automation, some industries continue to rely heavily on human labour. For example, garment, apparel, and footwear manufacturing remain labour-intensive sectors. These industries require fine motor skills and dexterity that machines cannot yet replicate cost-effectively. Similarly, in many other low-wage sectors, such as fish processing or agricultural work, technologies cannot compete with low labour costs. This suggests that while automation can substitute for certain tasks, it has limitations caused either by economic barriers (where the cost of robots outweighs the cost of humans) or because some work requires human judgment and adaptability, which technology is not yet capable of doing.

Technological progress cannot be stopped, nor should it be. Technology has the potential to make work safer and more fulfilling by eliminating repetitive and demeaning tasks. But at the same time, technology can put people out of work or devalue their labour. States and businesses can ensure labour is protected and human rights respected in the process of adopting new technologies.

Case Study: AI Opening Doors for People with Disabilities to Join the Workforce

Meet Suzy, a young deaf professional, and Alex, who is blind. Suzy always dreamed of a career in marketing, but traditional office meetings felt like a wall: she couldn't keep up with fast-paced conversations without straining to lip-read. Then her company introduced AI-powered real-time captioning tools, such as Ava and Microsoft Teams' live captions. Suddenly, every word spoken in a meeting appeared instantly on her screen as accurate text. "It changed everything," Suzy might say. "I could contribute ideas just like everyone else, without asking people to repeat themselves." This simple technology removed communication barriers, allowing her to shine in team discussions and advance in her career.

Across town, Alex, who lost his sight years ago, wanted to work in data analysis, a field full of charts, emails, and documents. Before AI, that seemed impossible. But tools like Seeing AI (from Microsoft) and smart glasses such as Envision or Meta Ray-Bans use cameras and voice descriptions to "read" the world around him: describing images, scanning text from screens or papers, and even identifying objects. At his desk, screen readers enhanced with AI summarise long reports or navigate complex spreadsheets aloud. For Alex, remote work became easier too, AI voice assistants handle scheduling and research. "Technology gave me independence and confidence," he shares in stories like his. "Now my disability doesn't hold me back; it just makes my approach different."

These examples, drawn from reports by the OECD and ILO, show how thoughtfully designed AI promotes inclusion. It reduces bias in hiring by focusing on skills (not appearances), adapts jobs to individual needs, and creates accessible environments. From a human rights perspective, this supports the rights to work (ICESCR Article 6) and to non-discrimination (Article 2), as well as the UN Convention on the Rights of Persons with Disabilities. When companies and developers involve disabled people in creating these tools, AI doesn't just automate, it empowers, turning potential obstacles into opportunities for dignity and equality in the workplace.

5.2 Human Rights in the Digital Workplace

As discussed, artificial intelligence and automation have reshaped how we think about human labour and the workplace. These changes have impacted human rights, specifically the right to work, the right to social security, the right to equality and non-discrimination and the right to privacy. This section discusses these human rights implications.

5.2.1 Right to Work

The right to work is recognised as a human right in Article 6 of the International Covenant on Economic, Social, and Cultural Rights (ICESCR). This right recognises that every individual can choose or accept employment without coercion, allowing them to lead a dignified life and fostering personal development within the community. It also encompasses the right to just and favourable working conditions, including safe workplaces (ICESCR Article 7), freedom to form and join trade unions, and protection against unfair dismissal.

However, technological advancements, particularly AI-driven automation, pose a significant challenge by displacing workers, leading to increased unemployment. Roles characterised by repetition, high precision requirements, and high-risk environments in sectors such as manufacturing and mining are increasingly susceptible to displacement by intelligent systems. This raises the legal question of whether employment termination due to technological change violates the right to work. The ILO's standards, set out in the *Convention on Termination of Employment,* **s**tate that employment should not be terminated without a valid reason, such as the worker's capacity, conduct, or the organisation's operational requirements. While businesses may cite cost-cutting as a reason, some argue that unregulated automation undermines the right to work. In current practice, most businesses can and do terminate workers' contracts if a robot replaces them.

From a legal perspective, the *Committee on Economic, Social and Cultural Rights (CESCR)* has established the doctrine of "non retrogression" (or not taking backwards steps), which generally forbids States from allowing more ESCR violations to occur. However, retrogressive steps, such as job replacement due to automation, may be permissible, according to the ICESCR Committee, if "duly justified by reference to the totality of the rights provided for in the Covenant." This means that states might prioritise other fundamental rights, such as the right to enjoy the benefits of scientific progress, over immediate employment preservation, particularly when automation or AI is beneficial to social development. Crucially, any such balancing act requires states to demonstrate that these measures serve the broader realisation of human rights, utilise all available resources effectively, and actively assist affected individuals with alternative employment opportunities, retraining programs, and adequate social protection during transition periods.

Case Study: AI-Driven Job Displacement in Asia-Pacific Economies

The UNDP's 2025 report, "The Next Great Divergence: Why AI May Widen Inequality Between Countries," highlights how artificial intelligence is reshaping labour markets in Asia and the Pacific, potentially exacerbating unemployment and inequality. Drawing on data from countries such as India and Indonesia, the report notes that AI could boost GDP growth by 2% annually through automation in sectors such as finance and healthcare, creating new digital jobs in data management and AI ethics.

However, it warns of massive disruption: nearly all jobs will be affected, with 40-60% of roles in routine tasks (e.g., clerical or service work) highly exposed to automation, potentially leading to a 5% decline in youth employment. Women and informal workers—comprising 73% of India's jobs and 59% in Indonesia—face heightened risks, as AI complements high-skill roles while displacing entry-level ones, widening generational and gender divides. This "divergence" favours advanced economies like Singapore, where skilled workers adapt quickly, over less-prepared nations like the Philippines, where limited digital access hinders reskilling. From a human rights lens, this threatens the right to work (ICESCR Article 6) by eroding access to dignified, stable employment, forcing workers into precarious gig roles without protections, and violating non-retrogression principles if states fail to mitigate losses through social safety nets or training.

5.2.2 Social Security Protection

Social security protection is universally recognised as a human right in the *Universal Declaration of Human Rights* (UDHR) Articles 22 & 25 and the *International Covenant on Economic, Social, and Cultural Rights* (ICESCR) Article 9. This right ensures that individuals can access benefits without discrimination when they lose work income due to various circumstances, including sickness, disability, pregnancy, work injuries, unemployment, old age, or the death of a family member. It also provides crucial protection from unaffordable healthcare costs and offers essential support to families, promoting decent working conditions, reducing poverty and inequality, and fostering economic stability.

However, achieving adequate and sustainable social protection consistently presents challenges in Southeast Asia, particularly for informal workers, vulnerable groups, and unregistered populations, primarily due to underfunded systems and fragmented national approaches. The situation is even more complex for platform economy workers – those employed through digital platforms like food delivery or ride-sharing services. These workers are often classified as self-employed, which typically excludes them from traditional employee-based benefits and places the full burden of social security contributions on the individuals themselves. Furthermore, irregular working patterns, diverse income streams, and the absence of employer contributions create significant barriers for these workers to meet eligibility thresholds and access adequate coverage. The online nature of platform work also contributes to a lack of collective worker organisations, leaving them particularly vulnerable without traditional forms of workplace representation and advocacy.

Both the G20 and ASEAN recognise these substantial gaps in social security coverage and financing within their member economies and call for stronger, more resilient, and sustainable social protection for all types of employment, including digital platform workers. For instance, Indonesia has introduced initiatives such as independent membership in social security schemes, allowing individuals who work independently, including platform workers, to pay for full membership and gain social security coverage.

Case Study: The Hidden Boss – Life as a Beverage Delivery Rider

Imagine a young man named Andi, weaving through the chaotic traffic of Tangerang on his motorbike, helmet on, phone mounted, delivering cold drinks on a sweltering day. Like hundreds of thousands of gig workers in Indonesia, Andi turned to a popular multinational beverage delivery app because it promised something priceless: flexibility. “Be your own boss,” the ads said. Log in whenever you want, work as much or as little as you like, and earn money on your terms, perfect for students, parents, or anyone needing extra cash in a country where formal jobs are scarce.

But as researchers Saifudin Asrori, Muhammad Isma’il, and Eve Gamalinda discovered in their 2025 study, “The Flexibility Illusion,” the reality for Andi and 19 other riders they interviewed was very different. Behind the cheerful app interface lurked an invisible, all-powerful boss: the algorithm.

Every morning, the algorithm decided who got orders, acting as a “gatekeeper” by checking ratings and performance scores. One low customer review (maybe for a late delivery caused by traffic) could drop your score, leading to orders vanishing without explanation. “The app decides everything,” one rider told the researchers. “Sometimes there are no orders for no clear reason.” To chase bonuses and stay visible, riders like Andi felt forced to work 10–12 hours a day, racing dangerously fast while the app tracked their every move via GPS. Earnings swung wildly; one good week might cover rent, the next barely paid for fuel and bike repairs. There was no sick pay, no health insurance, and no safety net if injured.

Women faced extra hardships. One rider, a mother, explained the “double burden”: long hours on the road, then rushing home to cook and care for children, avoiding risky night shifts that paid better. The constant pressure caused anxiety, “ratings are like ghosts haunting you”, and exhaustion, yet quitting meant no income at all.

The researchers called this “digital Taylorism”, a high-tech version of old factory management where workers are monitored, rated, and controlled without mercy, but now the risks (accidents, low pay, burnout) fall entirely on the rider. Platforms call them “independent partners” to avoid giving employee benefits, leaving workers vulnerable in Indonesia’s informal economy.

Andi's story, echoed by millions across the gig world, shows how technology that promises freedom can quietly erode human rights: the right to fair wages and rest, social security, privacy from constant tracking, and protection from discrimination. It reminds us that true progress means designing apps that respect dignity, not just profits.

In 2025, Malaysia's Parliament passed the landmark Gig Workers Bill, extending social protection to approximately 1.2 million platform workers in ride-hailing, delivery, and other gig sectors, a workforce that grew rapidly post-COVID but previously operated without formal employment rights. The Bill regulates service agreements, establishes the Malaysian Gig Economy Commission (SEGiM) to oversee the sector, and mandates contributions to social security schemes such as SOCSO (for injury and disability), while addressing calls for mandatory EPF retirement savings. Praised by unions and business groups as balanced, the legislation reflects state efforts to adapt regulations to the digital labour market, reducing precarity while supporting innovation in a sector vital to Malaysia's economy.

5.2.3 Disctimination and Algorithmic Bias

In the digital workplace, discrimination takes on new forms, particularly through algorithmic bias. Discrimination is defined in most human rights treaties, as well as in the ILO Convention. Workplace discrimination is understood as any unfavourable treatment based on legally protected characteristics such as race, ethnicity, colour, or gender that undermines employment equality. While some argue that technological tools can liberate decision-making from human bias and thus reduce discrimination, this perspective overlooks the possibility that the human intelligence embedded in AI technologies may itself be biased and generate new forms of discrimination.

Algorithmic bias refers to systematic, replicable errors in computer systems that lead to unequal and discriminatory outcomes, often stemming from biased training data. A prominent example is Amazon's AI recruiting tool, developed in 2014 to streamline the hiring process. This tool was found to be biased, prejudiced against female candidates, because it was trained on a decade of resumes predominantly from male applicants, leading it to penalise resumes that included the word "women" or were associated with women's colleges. The consequences of such bias are severe, including limited career opportunities for qualified candidates, perpetuation of systemic inequalities in the workplace and society, and reduced diversity and innovation within companies. Similar discriminatory tendencies have been found in other AI applications, such as creditworthiness assessments and agricultural recommendations.

The *ASEAN Guide on AI Governance and Ethics* explicitly acknowledges these risks of technological discrimination. It advocates for ethical safeguards to prevent algorithmic decisions from exacerbating existing social inequities, emphasising that AI system design, development, and deployment must align with principles of fairness and equity to ensure they do not perpetuate or amplify social disparities.

5.2.4 Privacy and Confidentiality

The human right to privacy protects personal autonomy and individual identity from external interference. Restrictions on privacy are permissible only when lawful, non-arbitrary, and in compliance with international human rights standards. In the digital workplace, new technologies create serious privacy concerns. Employers increasingly use AI and data tools to manage workers and make automated decisions about hiring, promotions, and firing. With the growth of the digital economy, workplace monitoring has expanded beyond traditional office settings into workers' personal lives, creating significant privacy risks. This can occur when work data is collected and mixed with personal information, including even sensitive details about workers' health. This phenomenon, known as "function creep," occurs when companies use data for purposes they didn't originally intend, leaving employees with almost no privacy. A common example of this is when a company searches a job candidate's social media before offering them a position.

Other examples of workplace surveillance include tracking digital communications such as emails and browsing history, monitoring keystrokes and screen activity, and using AI tools to analyse employee emotions. Biometric surveillance, such as fingerprint or face scanning, is common for attendance tracking and security, while GPS tracking monitors employee locations, particularly in logistics and delivery services like Gojek, Grab, or Foodpanda. These systems record location, delivery times, and response rates, and deviations can lead to

fewer jobs or suspension. Marginalised groups, especially low-income workers or those in precarious employment, are particularly vulnerable to such intrusive monitoring. They often feel pressured to accept it as a condition of employment, fearing job loss or retaliation, and may not fully understand how the system works or have avenues to challenge unfair treatment.

Data protection is one way to reduce threats to the right to privacy. Data protection concerns the safeguarding of any information related to a living person. Such information includes names, dates of birth, photographs, video footage, email addresses, telephone numbers, location data, biometric information as well as IP addresses and communication content.

Case Study: Always Being Watched – Surveillance in the Warehouses

Picture Maria, a warehouse worker at a large e-commerce fulfilment centre. She starts her shift scanning items at lightning speed, knowing that every movement is tracked: cameras overhead, scanners timing how long she takes per box, and algorithms calculating her "rate"—the number of packages handled per hour. If she slows down for even a moment—to stretch a sore back or grab water—she risks a warning or even losing her job.

The e-commerce fulfilment system, praised for efficiency, uses advanced surveillance technology to enforce strict quotas. Workers report feeling like they're in a "prison" or under "slavery-like" conditions. The constant monitoring leads to skipped bathroom breaks, high injury rates (workers push through pain to meet targets), and intense stress. One employee likened it to "being treated worse than robots." Women and workers of colour, who make up a large part of the warehouse workforce, face extra burdens from this pressure.

This intensive algorithmic surveillance raises serious human rights concerns: it invades privacy through non-stop tracking (ICCPR Article 17), undermines safe and fair working conditions (ICESCR Article 7), and jeopardises health and rest by prioritising speed over well-being. Critics argue it suppresses union organising by creating fear and erodes dignity, turning human labour into data points for profit.

5.2.5 The Right to a Healthy Work Environment

As AI systems and automation technologies expand across workplaces, they generate a growing but often overlooked problem: electronic waste (e-waste). While debates on AI frequently focus on fairness, bias, or job loss, far less attention is paid to the working conditions of those who handle the physical remains of digital technologies. From a human rights perspective, this issue directly engages the rights to safe and healthy working conditions and to a healthy environment, both of which are essential components of labour protection.

E-waste includes discarded computers, servers, sensors, batteries, industrial robots, and microchips, core components of AI and automated systems. These materials contain hazardous substances, including lead, mercury, cadmium, lithium, and rare-earth metals. When companies rapidly replace AI hardware to maintain speed and efficiency, large volumes of outdated equipment are discarded. Much of this waste ends up in low- and middle-income countries, where it is processed under unsafe and informal labour conditions.

For workers in informal e-waste recycling sectors, technology-driven waste creates serious occupational health risks. Many dismantle electronic components by hand, burn cables to extract metals, or use acid baths to separate valuable materials, often without protective equipment or proper ventilation. These practices expose workers to toxic fumes and dangerous chemicals, leading to respiratory illness, neurological damage, skin burns, cancer risks, and long-term reproductive harm. In some cases, children are involved in these activities, raising further concerns about child labour and violations of the right to health.

AI and automation intensify these labour risks in two main ways. First, the lifecycle of AI hardware is becoming shorter, as companies frequently upgrade servers, GPUs, and data-centre equipment. Second, the rapid growth of smart devices, sensors, robotics, and platform-based technologies in factories, warehouses, and delivery services increases the overall volume of hazardous waste that workers must handle. As a result, technological progress at one end of the supply chain creates dangerous and precarious work at the other. Communities living near informal recycling sites also face polluted air and water, further undermining their rights to health and adequate living standards.

Some Southeast Asian countries have begun to respond. Malaysia and Singapore have introduced extended producer responsibility schemes, while Vietnam and Indonesia have piloted formal recycling centres that offer safer conditions and more stable incomes for workers. However, informal recycling remains widespread, and enforcement is uneven. Ultimately, if AI-driven innovation depends on labour conditions that expose workers to toxic harm, then technological progress comes at the cost of human rights. Protecting workers from the dangers of e-waste is therefore not an environmental luxury, but a core labour and human rights obligation

5.3 Obligations

Ensuring that technological innovation impacting human labour aligns with human rights principles demands that both states and corporations respect and protect human rights and have mechanisms to prevent violations. They have distinct but interconnected legal obligations in the automated age. Under international human rights law, states have legally binding duties to promote and protect human rights, regardless of the type of work done. Corporations are required to uphold their responsibility to respect human rights, as found in the UN Guiding Principles on Business and Human Rights (UNGPs). They do this by conducting human rights due diligence (HRDD), knowing and showing their human rights obligations, and providing accessible grievance mechanisms under the three pillars of the UNGPs: Protect, Respect, and Remedy. Understanding these duties will help mitigate risks such as job displacement, algorithmic bias, and privacy violations.

5.3.1 State Obligations

Under the ICESCR, States have the duties to respect, protect, and fulfil rights. To respect, protect and fulfil means:

- The obligation to respect requires states to refrain from directly violating or impeding the exercise of human rights, demanding governmental restraint and non-interference.
- The obligation to protect means states should protect people in their jurisdiction from human rights violations by anyone, not just states. This includes corporations and non-state actors, necessitating robust legal and institutional mechanisms.
- The obligation to fulfil requires states to ensure that economic and social rights, which are not yet fulfilled, such as adequate housing or fair wages, will be realised through proactive and deliberate actions, such as the creation of enabling environments, supportive policies, and the allocation of necessary resources.

States play a pivotal role in shaping comprehensive standards that integrate human rights law into technological advancement. These responsibilities operate at both the national and international levels. At the national level, states must adopt new legislation, reform outdated laws that conflict with human rights standards, and establish clear operational boundaries for technology producers and corporations. This includes defining legal practices, developing frameworks to protect human rights, and ensuring legal consequences for private actors who commit violations.

In the context of the digital labour environment, these obligations are critical. States must develop regulatory frameworks that address the challenges of digitalisation, protect workers in automated settings and eliminate exploitation risks enabled by technological tools. Moreover, they must encourage the private sector and other stakeholders to respect human rights in line with the UN Guiding Principles on Business and Human Rights and domestic laws. Equally important is the duty to ensure that victims of violations have access to effective remedies, that threats or acts of violence are properly investigated, and that perpetrators are held accountable in order to combat impunity.

A key question is whether states should halt automation or restrict the use of artificial intelligence (AI) and digital platforms. But given that the technology is already used, it is not possible to abandon i; the focus should be on how it can be implemented responsibly. Automation, which gained momentum in the 1980s and accelerated during the COVID-19 pandemic, is often adopted to maintain economic competitiveness, even though it may disrupt employment. States should adopt approaches such as targeted restrictions, industry-specific guidelines, and balanced implementation. For example, automation could be permitted in export-oriented manufacturing, while restrictions might be imposed in labour-intensive domestic service sectors like retail, food service, and transportation. Such strategies enable technological efficiency without undermining people.ytilibats cimonoce dna laicos rieht dna krow s‘

5.3.2 Corporate Responsibility

In the digital age, corporate responsibility to respect human rights has taken on new dimensions and importance through the *UN Guiding Principles on Business and Human Rights* (UNGPs). These principles establish that businesses must avoid infringing on human rights and address any adverse impacts they cause. While digitalisation is being applied across all sectors, it has amplified existing risks and created unique challenges.

Technology companies and employers using AI or surveillance systems must consider how their operations and platforms impact human rights, particularly freedom of expression, privacy rights, and the fair treatment of workers. Businesses collect, process, and use vast quantities of data, and their technologies fundamentally shape how people work, communicate, and access essential services, underscoring this heightened responsibility. Respecting human rights in the digital era means that safeguards should be in place throughout business operations. This involves:

- Human rights due diligence: Companies should conduct rigorous assessments when developing or adopting new technologies, such as AI, facial recognition, or algorithmic decision-making, to systematically identify, prevent, mitigate, and address human rights risks.
- Knowing and showing human rights obligations: Businesses must understand and disclose the human rights implications of their technologies. Transparency fosters trust. Human Rights statements are becoming a common part of business accountability, and they demonstrate that businesses have done their homework on the rights implications of their work, whether that is the development or use of their technological tools
- Grievance mechanisms: Establishing accessible mechanisms to address complaints and provide remedies to individuals or communities harmed by their operations is crucial for reinforcing accountability and demonstrating a commitment to ethical practices. A mechanism allows affected stakeholders, including communities, to engage in meaningful dialogue with companies

The UNGPs alone are not the answer to ensuring business accountability. They are non-binding and rely on voluntary adherence. There are limited ways to ensure enforcement and accountability. Competitive pressures and business culture prioritises profit over human rights considerations, especially in tech sectors where regulation lags behind innovation and there is a race to innovate.

Case Study: Invisible "Ghost Work" in Southeast Asia and the Global South

Many AI systems that appear fully automated, such as chatbots, content moderators, search engines, and recommendation algorithms, actually rely heavily on hidden human work. Thousands of low-paid workers perform repetitive "micro-tasks" like labelling images, transcribing audio, cleaning datasets, and checking AI outputs for errors. This work is essential: without it, most AI models would not function accurately. Yet these workers remain largely invisible, rarely credited, poorly paid, and without job security or benefits. This "invisible labour" creates serious human rights concerns as follows:

Poor working conditions: Workers often earn below living wages, face intense time pressure, and experience psychological stress (especially content moderators exposed to disturbing material).

Lack of recognition and dignity: By presenting AI outputs as purely machine-made, companies hide the human effort behind them, treating workers as disposable.

Global inequality: Much of this work is outsourced to countries in the Global South, where labour is cheaper, reinforcing North-South divides.

In the Philippines, Indonesia, and Vietnam, thousands of workers support major AI platforms through companies like Appen, Scale AI, and local subcontractors. A 2025 study on platform-based data work in Indonesia found that workers labelling data for self-driving cars or training language models earn as little as US$1–3 per hour, with no health insurance or paid leave. Many are young people or women working from home, juggling micro-tasks around family responsibilities. One Indonesian worker interviewed said, "We are the ghosts making the AI look smart, but if we complain, we just get deactivated." Similar patterns exist in the Philippines' large BPO (business process outsourcing) sector, where workers moderate social media content for global tech firms under strict non-disclosure agreements, hiding both their role and the emotional toll of the job.

This violates the right to just and favourable conditions of work (ICESCR Article 7) and social security (Article 9). It also deepens inequality, as AI profits flow to companies in the Global North while risks are shifted to vulnerable workers in Southeast Asia.

Reflection and Discussion:

- *Does outsourcing data-labelling work to low-wage countries in Southeast Asia amount to modern exploitation?*
- *Should governments require tech firms to disclose how much human labour supports their AI systems and guarantee minimum standards for those workers?*
- *As AI improves, will invisible labour disappear or simply move to new hidden tasks? How can we ensure technological progress benefits workers in the Global South rather than exploiting them?*

5.3.3 Accountability Challenges in AI-Driven Labour

As AI systems increasingly shape how work is organised, evaluated, and even terminated, the question of who is responsible when things go wrong has become one of the most difficult issues in labour and human rights. When an AI tool produces a biased shortlist of job candidates, unfairly downgrades a platform driver's rating, or silently reallocates call-centre workloads in ways that harm workers' health, it is rarely clear where to place blame. Employers may point to the software vendor, vendors may blame the data, and governments may say the law has not yet "caught up" with technology. Yet from a human rights perspective, especially the rights to work, non-discrimination, and just and favourable conditions of work, this diffusion of responsibility is deeply problematic. Rights cannot be effectively protected if harms are treated as the fault of an "algorithm" rather than the humans and institutions that design, purchase, deploy, and profit from it.

Legally and ethically, this is often framed as a problem of attribution of liability. In traditional workplaces, if a manager discriminates in hiring or a supervisor sets unsafe workloads, responsibility is relatively clear. With AI, however, decisions are mediated by complex systems involving multiple actors: developers who build the model, data companies that supply training data, platform operators that integrate AI into their apps, and employers who rely on AI outputs in human resource decisions. In Southeast Asia's platform economy, for example, food-delivery and ride-hailing drivers in Indonesia and the wider region have described how opaque algorithms decide who gets jobs, how far they must travel, and when they may be suspended, often without meaningful explanation or effective appeal mechanisms.

Governance debates in the region are beginning to respond to these tensions. In Malaysia, the 2025 Gig Workers Bill amongst others prohibits unilateral rate changes and arbitrary account deactivations. In Singapore, the Ministry of Manpower has stressed that, regardless of the tools used, employers remain fully bound by the Tripartite Guidelines on Fair Employment Practices and the forthcoming workplace fairness legislation. If an employer uses AI in a way that results in discriminatory hiring or promotion, authorities can still act against the employer; the "blame the algorithm" defence does not apply.

These examples show how regulation can help re-anchor accountability in human decision-makers, even when AI is involved. The following case studies highlight how technological advancements, particularly in Artificial Intelligence (AI) and data management, can significantly impact employment, privacy, and social security.

Case Study: AI to Replace Roles at DBS, Southeast Asia's Largest Bank

DBS, recognised as Southeast Asia's largest bank, announced plans in February 2025 to replace approximately 4,000 jobs over the next three years as Artificial Intelligence assumes tasks traditionally performed by humans. These affected positions are primarily temporary and contract roles across the bank›s 19 markets, with the reduction expected to occur through natural attrition as projects conclude, ensuring permanent staff remain unaffected. This strategic shift is part of DBS›s long-term vision, which has seen the bank deploy over 800 AI models across 350 use cases, projected to generate an economic impact exceeding S$1 billion by 2025. While about 1,000 new AI-related positions are anticipated, this transition still signifies a notable displacement within the bank›s workforce, including 8,000 to 9,000 temporary and contract workers out of approximately 41,000 employees.

Reflection and Discussion:

- *Given DBS's plan to replace a substantial number of roles with AI, what are the primary human rights implications for its workforce?*
- *Because many workers are temporary and contract workers, is this good because they are not full-time, or is this bad because it is always the marginalised workers who lose their jobs?*
- *Are the UN Guiding Principles on Business and Human Rights relevant here? Is it accurate to say that the State has a duty to protect the rights of workers, and that DBS has a duty to respect its workers' rights? If yes, can you think of some of the actions that the State and DBS could take to address the situation?*

5.4 Conclusion

This chapter analyses technology's transformative impact on labour. It highlights the effects on the workforce, including job replacement and the emergence of new work models like the platform economy, which brings both benefits and challenges, such as uncertain employment status, limited social protection, and weakened collective bargaining for platform workers. The chapter details the human rights implications in the digital workplace, addressing the right to work (threatened by automation), the need for social security protection (especially for informal and platform workers), the prevalence of discrimination and algorithmic bias (such as in recruitment), and concerns for the right to privacy and data protection due to workplace surveillance and "function creep". It concludes by emphasising the state's obligations to respect, protect, and fulfil human rights in digital labour environments, and corporations' responsibility for human rights due diligence, transparency, and accessible grievance mechanisms.

Key Takeaways

1. AI does not just replace routine jobs; it changes the nature of almost every job.
2. Platform workers (ride-hailing, delivery, online freelancing) are often lose social security, stable income, and collective voice.
3. Algorithmic management brings extreme surveillance and stress into daily work life.
4. Bias in hiring and performance AI violates the right to non-discrimination.
5. States must protect and fulfil labour rights even when work is mediated by apps and robots; companies must respect rights through due diligence.
6. Upskilling, portable social protection, and worker-owned platforms are already proving that a rights-respecting automated future is possible.

Issues to Think About

1. If a robot or AI takes your future job, do you believe the government owes you retraining and income support? Why or why not?
2. When you order food late at night, do you think about the rider's working conditions controlled by the app? How could you act on that thought?
3. Would you accept lower privacy at work (constant tracking, mood monitoring) in exchange for higher pay? Where would you draw the line?
4. Should gig workers be automatically classified as employees with full rights, or is "flexibility" worth the trade-off?
5. Name one skill you could learn this year that would make you harder to replace by AI—and also more valuable to society.
6. Ten years from now, do you want to live in a world with a universal basic income because AI took most jobs, or a world where every new technology is required to create at least as many decent jobs as it destroys? Which future are you willing to fight for?

Further Readings

FerMUN. (2024). *How can we protect workers in the face of the rise of artificial intelligence, to ensure that jobs are preserved and their rights respected?*https://fermun.org/wp-content/uploads/2024/11/ILO4_Research-Report_-A.I-_-workers-rights_EN.pdf

International Economic Development Council. (2025). *Artificial intelligence impact on labor markets: Literature Review*. https://www.iedconline.org/clientuploads/EDRP%20Logos/AI_Impact_on_Labor_Markets.pdf

International Labour Organization. (2022). *Technological Progress and the Dynamics of Self-Employment: Worker-level Evidence for Europe*. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_emp/documents/publication/wcms_837902.pdf

International Labour Organization. (2025). *Generative AI and jobs: A refined global index of occupational exposure*. https://www.ilo.org/publications/generative-ai-and-jobs-refined-global-index-occupational-exposure

International Labour Organization. (2025). *Work transformed: The promise and peril of artificial intelligence*. https://www.ilo.org/publications/work-transformed-promise-and-peril-artificial-intelligence

International Trade Union Confederation. (2025). *Artificial Intelligence and Digitalisation: A matter of life and death for workers*. https://www.ituc-csi.org/IMG/pdf/ituc_workers_memorial_day_report_2025_final.pdf?42357/8ae22358d52b46270b50634cd58f0bf7d2e8735977a52f4dc87fc139a1a172a1

National Disability Institute. (2025). *The intersection of technology, disability rights and worker rights*. https://www.nationaldisabilityinstitute.org/wp-content/uploads/2025/01/intersectionoftechnologydisabilityandworkerrights2024report.pdf

Rindiani, N. S. (2025) The AI Paradox: Invisible Labor in the Age of Automation. Center for Digital Society. https://digitalsociety.id/2025/03/21/the-ai-paradox-invisible-labor-in-the-age-of-automation/19692/

Supply Chain Brain. (2025). *Labor rights, automation to reshape supply chain workforce in 2025*. https://www.supplychainbrain.com/articles/40862-labor-rights-automation-to-reshape-supply-chain-workforce-in-2025

The Employer Report. (2025). *Navigating labor's response to AI: Proactive strategies for multinational employers across the Atlantic*. https://www.theemployerreport.com/2025/06/navigating-labors-response-to-ai-proactive-strategies-for-multinational-employers-across-the-atlantic/

United Nation (2011), Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, . https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

World Bank Group (2025). Future Jobs: Robots, Artificial Intelligence and Digital Platforms in East Asia and Pacific, https://www.worldbank.org/en/region/eap/publication/future-jobs

Chapter 6:

Environmental Technologies and Human Rights

Reader's Guide

This chapter invites you to view environmental technologies not as neutral tools, but as innovations that can both safeguard our planet and pose risks to human rights in everyday life. From solar panels powering remote villages in the Philippines to AI-driven haze-monitoring apps alerting families in Indonesia, to geoengineering proposals that could alter weather patterns over the Mekong Delta, these technologies are reshaping how we combat climate change, pollution, and resource loss across Southeast Asia. In this chapter, you will discover why the same solutions that promise sustainability can also enable displacement, deepen inequalities, or harm vulnerable communities if not guided by rights principles. By the end, you will have the foundation to question the impact of environmental technologies (Envirotech) and advocate for solutions that prioritise justice, equity, and a healthy planet for all. In this chapter, you will:

- Understand Southeast Asia's environmental crises, from deforestation and haze pollution to climate-driven disasters—as human rights issues that threaten lives, livelihoods, and dignity.
- Learn key rights like the right to a healthy environment (RtHE), free, prior, and informed consent (FPIC), and intergenerational equity, and how they intersect with climate change and corporate accountability.
- See how Envirotech, from renewable energy and pollution sensors to geoengineering, can promote sustainability while aligning with frameworks such as the UNGPs and the Paris Agreement.
- Recognise common harms, such as e-waste health risks, Indigenous land grabs from "green" projects, and unequal access to tech benefits, and why they matter to you and your community.

Start thinking about your role in advancing rights-based envirotech, from local advocacy to holding governments and businesses accountable. Let's begin.

Key Terms

Climate Justice: The principle of ensuring equitable treatment and outcomes in addressing climate change impacts, prioritising fairness for vulnerable populations to promote social and environmental equity in policy and technology use.

E-Waste: Discarded electronic devices and components that, if improperly managed, release toxic substances, polluting soil and water and endangering human health and environmental integrity.

Free, Prior, and Informed Consent (FPIC): A right requiring that indigenous communities give their voluntary, informed agreement to projects affecting their lands or resources, ensuring their autonomy and cultural preservation.

Geoengineering: Deliberate, large-scale technological interventions in Earth's climate systems to mitigate environmental issues, such as altering weather patterns or carbon levels, with potential ecological and social consequences.

Human Rights and Environmental Due Diligence: A corporate responsibility process to identify, prevent, and mitigate adverse impacts on human rights and the environment caused by business activities or technologies.

Renewable Energy: Energy derived from naturally replenishing sources, such as solar, wind, or hydro, which reduces environmental harm and supports sustainable development, though implementation may raise land or resource issues.

Self-Determination: The right of communities, particularly indigenous groups, to freely govern their cultural, economic, and land-related affairs, ensuring control over their resources and heritage.

Transboundary Haze Pollution: Air pollution, primarily from fires, that crosses national borders, degrading air quality and posing health risks, requiring regional cooperation for effective mitigation.

6.1 Introduction: Overview of Southeast Asia's Environmental Challenges

Southeast Asia (SEA) is home to over 667 million people and amazing natural wonders such as the rainforests in Borneo, the emerald waters in Ha Long Bay, the colourful reefs of the Coral Triangle, to name just a few. However, the region also faces an environmental crisis. The geography of SEA makes it vulnerable to natural hazards such as cyclones, heavy rainfalls, earthquakes, tsunami and volcanic eruptions. Rapid economic growth and urbanisation in the region have also adversely impacted the environment. The tropical forests of SEA, one of the most biodiverse in the world, are disappearing at an alarming rate due to land conversion for palm oil plantations, infrastructure development and illegal logging. This biodiversity loss threatens countless species and disrupts the livelihoods of indigenous communities who depend on ecosystems for food, water, and cultural heritage.

The rapid decline of natural habitats undermines ecosystem services critical to human well-being and regional stability. In addition, water security is a pressing concern in SEA, where less than 30% of domestic wastewater is treated in most ASEAN countries. Untreated sewage and industrial effluents contaminate water sources, spreading diseases like leptospirosis. Marine environments face severe threats from plastic pollution, with SEA emerging as a global hotspot for plastic waste and overfishing. These issues harm coastal communities reliant on marine resources for their livelihoods and food security. The rise of waste streams, such as electronic waste and plastics, creates significant environmental and health challenges. Toxic substances, like mercury from illegal mining, pose risks including neurological damage. Poor waste management systems and inadequate regulations exacerbate these problems, leaving communities exposed to hazardous conditions.

Air pollution, particularly transboundary haze from forest and peatland fires, poses significant health risks across SEA. Urban centres like Jakarta, Manila, and Bangkok frequently exceed World Health Organisation (WHO) PM2.5 air quality standards due to vehicle emissions, industrial activities, and agricultural burning. This leads to chronic respiratory illnesses, reduced life expectancy, and substantial economic losses. The ASEAN Agreement on Transboundary Haze Pollution aims to address this issue but struggles with enforcement, limiting its effectiveness.

SEA is also among the world's most vulnerable regions to climate change. The frequency and intensity of natural calamities in the region have increased, threatening lives, livelihoods and habitats of people. Rising sea levels threaten millions in low-lying areas like the Mekong Delta and Jakarta, while stronger typhoons put the right to life and housing at risk in the Philippines and Vietnam.

Reflection and Discussion:

Grab a map of Southeast Asia (physical or digital) and mark key locations of environmental challenges and tech interventions, e.g., the dams, the deforestation, the polluted rivers, the smog centres, where there is overfishing or destruction of coral reefs, etc. Discuss:

- *How do these sites illustrate the link between environmental crises and human rights? What technologies could be deployed here?*
- *Examine the environmental challenges, their causes, and discuss the possible impact on human rights. For example, climate change and energy crisis pose threats to the enjoyment of the rights to life, health, and food security.*

Despite all these challenges, effective solutions are hindered by governance gaps, including unclear regulations, limited access to environmental data, and the suppression of environmental activists. These barriers impede progress and accountability. Regional cooperation is essential to address transboundary issues, but inconsistent policies and enforcement remain obstacles. Table 6.1 presents environmental challenges and key causes.

Table 6.1: Environmental Challenges and their Impacts to Human Rights

Environmental Challenge	Key Causes	Impacts on Human Rights
Climate Change & Energy Crisis	Fossil fuel reliance, subsidies, GHG emissions growth	Threats to life, health, food security; increased poverty
Air Pollution & Haze	Urbanization, forest fires, industrial emissions	Right to health violations (respiratory diseases)
Biodiversity Loss & Degradation	Deforestation, overexploitation	Loss of self-determination for indigenous groups; cultural erosion
Water & Marine Pollution	Untreated wastewater, industrial discharge	Rights to water, sanitation, health
Waste & Chemicals Management	Linear economy, e-waste surge	Health risks from toxins; environmental injustice
Governance Gaps	Data shortages, weak enforcement	Limited access to information, participation, justice

You Are Here: Environmental Crises are Personal

If you live in Southeast Asia, environmental crises are not distant or abstract. Haze may affect whether you attend class, floods may disrupt transport, and heatwaves may make daily life uncomfortable or unsafe. These experiences show why environmental problems are also human rights issues. They shape people's health, safety, and dignity in real and immediate ways.

6.2 Environment, Climate Change and Human Rights

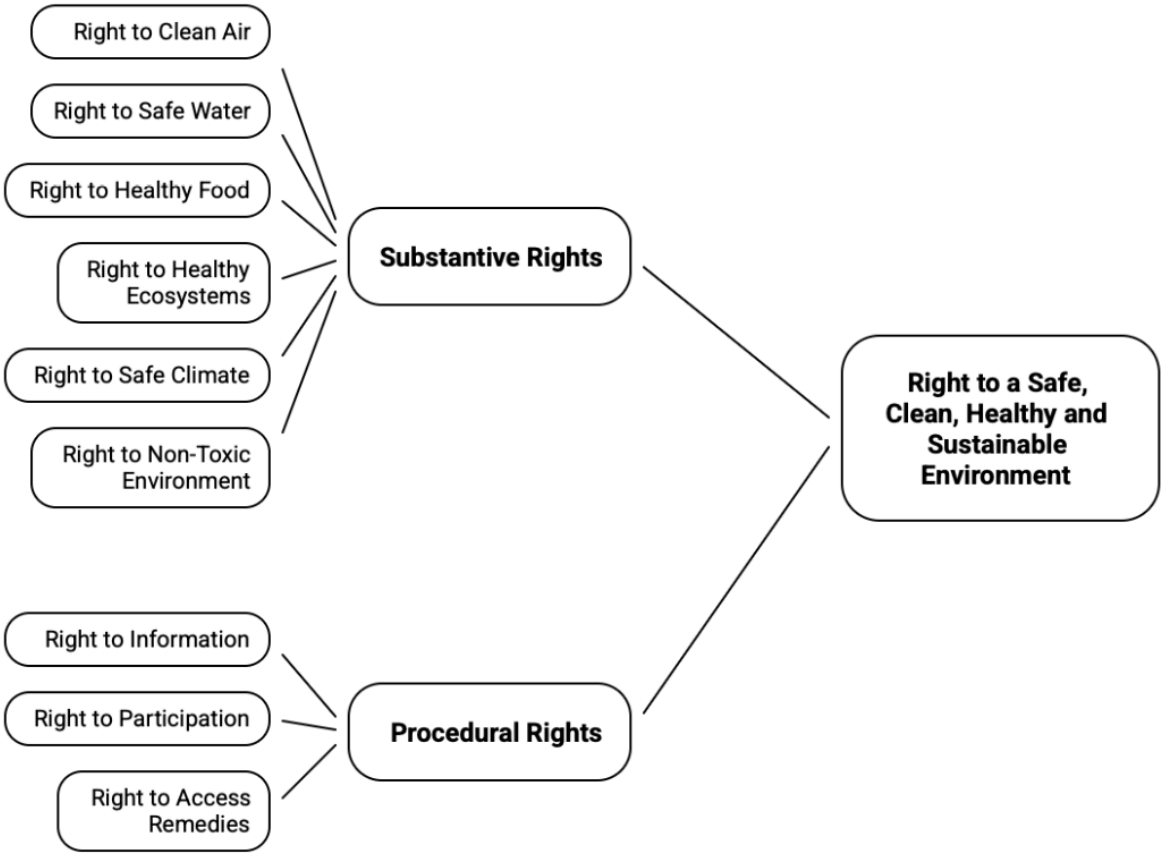
The necessity of establishing regulations and limitations on human use and abuse of the environment has become increasingly important as the impacts of environmental degradation and climate change threaten the very existence of our societies. This section examines the landscape of international law and standards on environmental protection and climate change.

6.2.1 The Human Right to a Safe, Clean, Healthy and Sustainable Environment

The link between environmental protection and human rights rests on the recognition that a clean, safe, and sustainable environment is a prerequisite for the full realisation of numerous human rights. The right to a safe, clean, healthy and sustainable environment has been recognised as a human right by the UN General Assembly in 2022. As illustrated in Figure 6.1, the right to a safe, clean, healthy, and sustainable environment has two components:

a) substantive rights, or environmental conditions that every individual is entitled to, and
b) procedural rights, such as rights that support environmental policy-making and governance.

Figure 6.1: Components of the Right to a Safe, Clean, Healthy and Sustainable Environment



Substantive rights

The Special Rapporteur on Human Rights and Environment, David Boyd, identified six elements of the substantive right to a safe, clean, healthy and sustainable environment:

- *Right to clean air:* All persons have the right to breathe air that is of acceptable quality and is free from pollutants. The right to clean air is interlinked with other rights such as the right to health and the right to life.
- *Right to safe and sufficient water:* All persons have the right to safe and sufficient water for their personal and domestic use. Pollution and pathogens make water unsafe for human consumption. Safe and sufficient water is also vital for healing the right to food, particularly those engaged in small-scale farming and fishing. Droughts and floods jeopardise the right to food.
- *Right to healthy and sustainably produced food:* Food is a necessity for life. Food also has an economic role, as it supports the livelihoods of a substantial percentage of the population. Environmental degradation and climate change negatively impact people's livelihoods. At the same time, the industrial food system, which encourages large monocultures, has the impact of decreasing agricultural biodiversity and jeopardising food security. Industrial agriculture also contaminates air, water and soil resources with synthetic fertilisers and other pollutants. Agriculture is also a major source of green house gasses (GHGs) through deforestation, gases from livestock such as cattle, and methane from rotting food waste
- *Right to healthy ecosystems and biodiversity:* Healthy ecosystems are the source of food, water, clean air, and biodiversity. Human rights ultimately depend on a healthy biosphere. Changes in land and sea use (such as the conversion of forests to agriculture or industry), exploitation of natural resources (such as logging, overfishing, and poaching), and climate change and pollution are among the causes of the decline in the health of our ecosystem.
- *Right to* a *safe climate:* Climate change, linked with other factors such as poverty and conflict, can lead to food insecurity, loss of livelihoods, forced displacement, and health and sanitation crises.
- *Right to* a *non-toxic environment that is free from pollution and toxic substances:* Pollution and toxic substances have an adverse impact on the right to health and a healthy environment in terms of diseases and premature deaths.

Procedural rights

The Convention on Access to Information, Public Participation in Decision Making and Access to Justice in Environmental Matters also known as the Aarhus Convention adopted in 1998 links government accountability with environmental protection. It recognizes that public participation is essential for protecting the environment and imposes obligations on public authorities regarding access to information, public participation and access to justice. The Convention is only binding for countries in the European Union, though a very small number of countries outside do recognize it. However, it has become the international standard for what are known as procedural environmental rights such as:

- *Right to information:* People have the right to access information related to the environment. States have the obligation to provide the public with accessible, affordable and understandable information. The right to information is linked with the rights to freedom of expression, association and peaceful assembly in environmental matters.
- *Right to participation:* People have the right to participate in decision-making on matters related to the environment. In order to facilitate such participation, States have the obligation to require assessments of the possible environmental and human rights impacts of proposed projects and policies. Such assessment studies should be made available to the public.
- *Right to access remedies:* All persons have the right to access effective remedies for violations of the right to a safe, clean, healthy and sustainable environment.

The right to a safe, clean, healthy and sustainable environment imposes obligations on States to respect, protect and fulfill the substantive and procedural components of the right. The obligation to fulfill requires States to establish, implement and enforce laws, policies and programs such that people can enjoy the right to a safe, clean, healthy and sustainable environment. Moreover, States must ensure that law and policy measures are adopted based on inclusive public participation and that information about such measures is available to the public.

Reflection and Discussion:

How does air pollution from daily traffic or household waste in your city affect your right to clean air and health? Share a personal experience where poor air quality impacted your day, and discuss ways communities could use apps or local policies to claim procedural rights like access to information.

6.2.2 Corporate Accountability

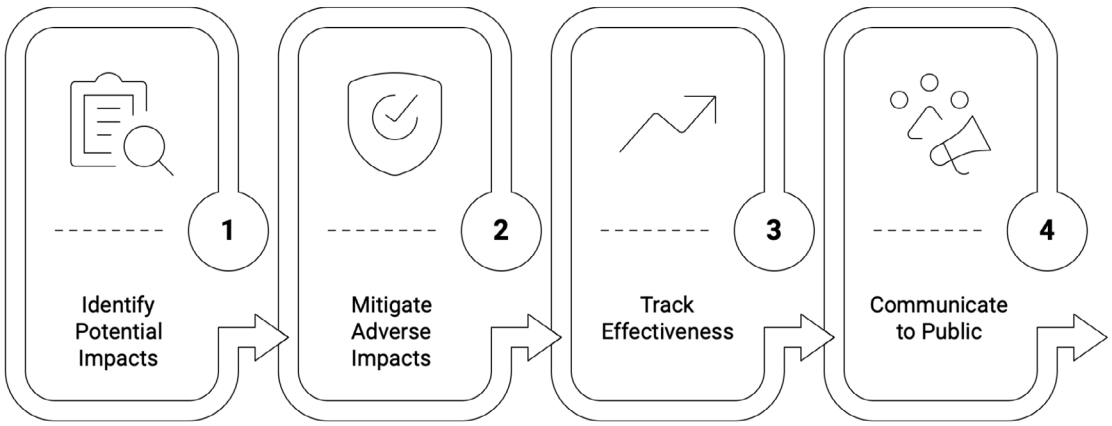
Corporate accountability refers to the responsibility of businesses to prevent and address adverse impacts their operations may have on individuals or communities, particularly human rights violations. The UN Guiding Principles on Business and Human Rights (UNGPs), also known as the Ruggie Principles, provide a framework for business conduct. They are structured around three pillars,

- The State's obligation to protect,
- Businesses' responsibility to respect, and
- The obligation to provide access to remedies.

Under these principles, corporations have the responsibility to respect human rights throughout their operations. One of the key elements of this responsibility to respect is human rights due diligence. The steps involved in human rights due diligence are summarised in Figure 6.2, which shows how companies identify risks, take action, track outcomes, and communicate their responses.

1) Identifying and assessing potential adverse human rights impacts;
2) Taking appropriate actions to mitigate the identified adverse impacts;
3) Tracking the effectiveness of the measures taken, and
4) Communicating to the public as to how potential adverse human rights impacts have been addressed.

Figure 6.2: Human Rights Due Diligence Process



Such human rights due diligence involves having meaning consultations with affected rights holders and other stakeholders. A common criticism of the UNGPs is their non-binding nature, meaning compliance often depends on corporate goodwill rather than legal obligation, limiting enforcement and accountability, especially when companies prioritise profit over ethical considerations in rapidly evolving technology sectors. This can lead to uneven implementation and gaps in protection for affected individuals. Responding to these inadequacies, the UN Special Rapporteur on human rights and the environment has suggested enactment of human rights and environmental due diligence laws that aim to identify, assess, prevent, cease, mitigate and effectively remedy potential and actual impacts of business operations on ecosystems and human rights, including the human right to a clean, healthy and sustainable environment.

Reflection and Discussion:

Think about a product you use daily, such as a smartphone or a fast-fashion item. How might its production involve environmental harm or human rights issues (e.g., e-waste from old devices)? Discuss how you, as a consumer, could push companies for better due diligence through boycotts or social media campaigns.

In your routine, do apps or gadgets from big tech firms (e.g., ride-sharing or food delivery) contribute to urban pollution? Explore how requiring corporate transparency reports could empower everyday users to hold businesses accountable for rights violations.

6.2.3 Free, Prior and Informed Consent (FPIC), Indigenous Peoples

Indigenous peoples, because of their strong connection to land and natural resources, are rendered most vulnerable by biodiversity loss and environmental degradation. Large-scale industrial activities, pollution of air, water and land resources, deforestation for agriculture or extractive mining, etc., pose a threat to their rights to life and livelihoods. The impact of climate change creates further challenges, pushing many indigenous groups towards forced migration.

The United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) adopted in 2007, recognises these challenges. Article 3 of the Convention recognises the right to self-determination of indigenous peoples to freely pursue their economic, social and cultural development. From this right to self-determination, other rights of indigenous peoples flow, such as the right to the conservation and protection of the environment (Article 29) and the right to participate in decision-making, imposing an obligation to seek free, prior, and informed consent before planning any project that impacts their rights. The standard of free, prior and informed consent (FPIC) is also reaffirmed in the International Labour Organisation Convention 169 (ILO 169), the Convention on Biological Diversity, 1992 (CBD), the due diligence framework under the UNGPs, and national laws.

6.2.4 UNFCCC, Paris Agreement and Climate Equity

The United Nations Framework Convention on Climate Change (UNFCCC), adopted in 1992, is the foundational international treaty addressing climate change. Its primary objective is to stabilise greenhouse gas concentrations at a level that prevents dangerous human-induced interference with the climate system. The Convention recognises that climate change threatens ecosystems, human well-being, and sustainable development, and therefore requires coordinated international action based on equity and shared responsibility.

Building upon this framework, the Paris Agreement was adopted in 2015 under the UNFCCC. The Agreement aims to limit the increase in global average temperature to well below 2°C and to pursue efforts to limit warming to 1.5°C above pre-industrial levels. These temperature targets are designed to reduce climate-related risks such as sea-level rise, extreme weather events, food insecurity, and forced displacement, impacts that disproportionately affect vulnerable populations.

To achieve these goals, States are required to submit Nationally Determined Contributions (NDCs). These are national climate action plans outlining each country's intentions to reduce greenhouse gas emissions and adapt to climate change. While the Paris Agreement allows flexibility based on national circumstances, it requires States to progressively increase ambition over time. Collective progress is assessed through a Global Stocktake, conducted every five years under Article 14, which evaluates whether global efforts are aligned with scientific findings and equity considerations.

Climate Equity, Environmental Justice, and Climate Justice

Importantly, international climate law does not treat climate change as a purely technical or scientific problem. Instead, it embeds principles of equity and justice, particularly through the Paris Agreement's Preamble. In climate governance, equity is commonly expressed through two closely related concepts: environmental justice and climate justice.

Environmental justice refers to the principle that all people, regardless of race, income, or social background, should be treated fairly and have a meaningful voice in environmental decision-making. A central concern of environmental justice is that no group should bear a disproportionate share of environmental harm. This principle is closely linked to environmental equity, as pollution and environmental risks are often concentrated in underserved or economically disadvantaged communities, such as those living near industrial zones, plantations, or waste disposal sites. Fairness, equality, and human dignity therefore lie at the heart of environmental justice, which also emphasises procedural rights such as access to information, public participation, and access to remedies. These procedural dimensions are particularly important for Indigenous peoples, whose lands and livelihoods are often directly affected by environmental decisions.

Climate justice, by contrast, focuses specifically on fairness in relation to the causes and impacts of climate change. Climate change is inherently unjust because States that have historically contributed the most to greenhouse gas emissions often have greater economic and technological capacity to protect themselves from its impacts. Meanwhile, poorer States and marginalised communities, who have contributed very little to global emissions, are likely to suffer the most severe consequences. Small island States face the risk of disappearing due to sea-level rise, while rural and coastal communities experience flooding, typhoons, droughts, and land degradation that undermine food security and livelihoods.

These justice-based principles are firmly recognised in international environmental law. Principle 1 of the Stockholm Declaration (1972) affirms that all humans are entitled to "an environment of a quality that permits a life of dignity and well-being." The Rio Declaration (1992) strengthens this commitment by emphasising equity, participation, and common but differentiated responsibilities, particularly through Principles 10 and 11. Similarly, Articles 3 and 4 of the UNFCCC emphasise the need to protect vulnerable communities, including developing countries and those most exposed to climate risks. The Preamble to the Paris Agreement further reinforces these ideas by explicitly recognising gender equality, intergenerational equity, and the empowerment of vulnerable groups.

Reflection and Discussion:

In climate events like heavy rains flooding your street, who in your community (e.g., elders or low-wage workers) suffers most? Relate this to climate justice and brainstorm everyday actions, like recycling drives, to ensure fair tech access.

Intergenerational and Gender Equity

Two equity principles deserve particular attention in climate governance: intergenerational equity and gender equity.

- *Intergenerational equity* recognises that present generations have a responsibility to ensure that their actions do not compromise future generations' ability to enjoy a safe, healthy, and sustainable environment. Climate decisions made today, such as delaying mitigation or continuing environmentally harmful practices, will shape the environmental conditions future generations inherit.
- *Gender equity* recognises that climate change affects women and men differently. Women often face greater vulnerability due to structural inequalities, including limited access to land, resources, and decision-making power. Climate-related disasters, food insecurity, and displacement tend to intensify these inequalities. By explicitly recognising gender equality, the Paris Agreement calls for inclusive climate policies that take into account the distinct experiences and needs of women.

REDD+ and Forest-Based Climate Mitigation

In addition to emission-reduction commitments under the Paris Agreement, the UNFCCC framework includes specific mitigation mechanisms, such as REDD+ (Reducing Emissions from Deforestation and Forest Degradation). REDD+ was developed to address emissions resulting from deforestation and forest degradation, particularly in developing countries where forests play a critical role in livelihoods, biodiversity protection, and climate regulation. The "+" refers to additional activities such as forest conservation, sustainable forest management, and enhancement of forest carbon stocks.

Under the REDD+ framework, countries may receive results-based payments for verified emission reductions achieved through forest protection and sustainable management. In theory, REDD+ offers a triple benefit: mitigating climate change, conserving biodiversity, and supporting local and Indigenous communities. However, from an environmental justice perspective, REDD+ also raises important concerns. If poorly designed, REDD+ projects may restrict access to forests, undermine customary land rights, or exclude Indigenous peoples from decision-making processes. This highlights the importance of applying procedural rights—particularly participation, transparency, and free, prior, and informed consent (FPIC)—in forest-based climate initiatives.

Case Study: The REDD+ Program and Human Rights Violations

In one case in Panama, the REDD+ program encroached upon the ancestral lands of the Ngäbe-Buglé Indigenous group, whose territory overlapped with the forests targeted for REDD+ interventions. Indigenous communal property rights were taken away so that the forests could be managed as a carbon sink. The program, intended to abate emissions, ironically limited Indigenous control over their ancestral territories. The authorities failed to obtain Free, Prior, and Informed Consent from the Ngäbe-Buglé people. Without Indigenous voices being included, such initiatives risk becoming a new means of land displacement and cultural genocide.

The reliance on remote monitoring technologies like satellites and data analytics by the government and its international partners was not adequately balanced with consultation or communication with affected communities. This top-down flow of information meant local communities were largely unaware of, or did not fully understand, the program's implications, leading to their exclusion from early involvement when they could have highlighted concerns. Such actions raised human rights issues related to the rights to participation and to access to information, specifically Article 6 of the Aarhus Convention.

The REDD+ case in Panama has ethical, legal, and social implications arising from the deployment of environmental technologies.

The case presented a dilemma on whether the environmental benefits of REDD+ justified infringing upon local communities' human rights. Critics questioned the program that effectively paid other actors to protect an ecosystem at the cost of respecting Indigenous rights, especially when the application of technology ignored the ethical principle of community consent. The exclusive focus on ecological sustainability without balancing it with the rights of the affected population, including potential threats to food security from limited access to Indigenous lands, are human rights concerns. Environmental technologies are not neutral mechanisms but tools of implementation that need to be guided by human rights.

From a legal standpoint, the program's actions were incompatible with several international standards. The violation of Indigenous land rights, particularly the absence of FPIC, directly contravened the UNDRIP (Articles 10 and 19). Furthermore, the lack of consultation and public participation violated the procedural rights guaranteed under the Aarhus Convention (Article 6). Even the Paris Agreement, while a climate treaty, notes that countries "should, when taking action to address climate change, respect, promote and consider their respective obligations on human rights", including indigenous peoples' rights, particularly in its preamble. The failure to consult in projects like Barro Blanco undermined international human rights standards and environmental law.

The REDD+ program also generated social mistrust between the government and Indigenous communities, which sparked protests and demands for greater transparency and respect for rights. The program's unilateral, top-down approach undermined relationships and eroded local support for broader environmental objectives. Indigenous communities felt concerned about losing lands they had historically managed. This exclusion led to disempowerment and dispossession, making it difficult to reach further agreements. This revealed a "tech-heavy" approach that focused more on data-driven compliance (such as deforestation rates) than on the human rights of Indigenous communities.

The REDD+ experience in Panama offers an important lesson for Southeast Asia, where many climate and forest protection projects rely on similar technologies such as satellite monitoring, carbon accounting, and digital land mapping. ASEAN countries like Indonesia, Malaysia, and the Philippines also have large forest areas that are home to Indigenous and local communities. This case shows that while envirotech can support climate goals and forest conservation, it can also violate rights if communities are excluded from decision-making. For ASEAN, the key lesson is that climate technologies must be implemented with strong safeguards for participation, transparency, and free, prior, and informed consent (FPIC). Without a rights-based approach, even "green" solutions risk repeating patterns of inequality and injustice in the region.

Reflection and Discussion:

1. *Should indigenous groups accept that, in order respond to climate change, they have to allow REDD+ "tech-heavy" activities because this will protect forests? Are the concepts of environment and climate justice relevant?*
2. *What are ways to rights-based actions that can help heal the social mistrust between the Indigenous groups and the Panama government after part of their land was taken over to be managed under REDD+?*
3. *Human rights and environmental due diligence should include identifying human rights concerns through a risk assessment. What are some example items in a risk assessment of a company which wants to manage forests which are near indigenous communities?*

Environmental Justice in Southeast Asia

At the regional level, environmental and climate justice are pressing concerns in Southeast Asia. Vulnerable groups, including women, children, Indigenous peoples, and rural communities, often experience the most severe environmental harms while benefiting the least from economic growth and technological development. Environmental degradation in the region frequently intersects with existing inequalities related to class, gender, ethnicity, and geography.

For example, women in rural communities who depend on fisheries for their livelihoods are disproportionately affected when upstream hydropower dams alter river flows and reduce fish stocks. Children living in urban informal settlements are exposed to higher levels of air pollution, leading to higher rates of asthma and other respiratory illnesses. These examples demonstrate how environmental harm is unevenly distributed and reinforces broader patterns of social exclusion.

A particularly severe consequence of climate injustice in Southeast Asia is climate-related mobility and displacement. Rising sea levels, coastal erosion, intensified storms, and environmental degradation are forcing communities to relocate, often infringing upon human rights such as the right to life, housing, culture, and self-determination. Displacement may also result in loss of livelihoods, breakdown of social networks, and limited access to legal remedies.

Vulnerable groups face compounded risks during displacement. Women and girls are more exposed to gender-based violence, while children experience disruptions to education and healthcare, deepening intergenerational inequalities. Indigenous peoples, particularly in coastal and forested areas, may lose ancestral lands, raising concerns about violations of FPIC and self-determination rights.

As climate impacts intensify, technology is increasingly promoted as a solution to environmental and climate challenges. International frameworks encourage States to act on the best available scientific evidence, including adopting sustainable technologies while discontinuing harmful practices, a process known as exnovation. The 2030 Agenda for Sustainable Development also emphasises the development and transfer of environmentally sound technologies.

In this context, environmental technologies (envirotech) offer important opportunities. AI-driven predictive modelling can improve early-warning systems and relocation planning, while satellite data is increasingly used in flood-prone regions of Southeast Asia. Blockchain technology has also been proposed to support transparent land registries and equitable resettlement processes. However, without inclusive governance, these tools risk deepening existing inequalities, particularly if biased data excludes marginalised communities.

Reflection and Discussion:

- *A government approves a large infrastructure project that boosts jobs and economic growth today. However, environmental experts warn it will increase emissions and damage ecosystems for decades. The project will likely still affect people who have not yet born. How does the principle of intergenerational equity help us evaluate whether such development decisions are fair?*
- *Following a severe flood, women in a rural community spend more time collecting clean water, caring for children and elderly family members, and rebuilding homes, while having little say in local recovery planning. Why does climate change often affect women more severely, and how should gender equity shape climate policies and disaster responses?*

International environmental and climate law sets important standards for protecting human rights, such as fairness, participation, and accountability. However, in everyday life, it is environmental technologies (envirotech) that often determine whether these rights are actually protected or violated. Technologies like renewable energy systems, pollution monitoring tools, and climate data platforms shape access to clean air, safe water, and climate protection. When these technologies are designed and used responsibly, they can support environmental justice. But when they are poorly regulated or exclude affected communities, they can worsen inequality and harm human rights. Understanding envirotech as a bridge between law and real-world experience helps us see why technology choices matter for human rights outcomes.

6.3 Environmental Technologies and their Integration in SEA

Environmental Technologies (Envirotech) refer to a wide array of innovations, both digital and non-digital, whose primary purpose is to reduce or prevent environmental harm, promote sustainable resource use, and decrease resource depletion. These technologies are specifically developed to manage the challenges of climate change, air and water pollution, and biodiversity loss.

You Are Here: You Already Use Envirotech

When you check an air-quality app, follow flood alerts on your phone, or see satellite images of forest fires online, you are already interacting with environmental technologies. These tools influence how you behave, how governments respond, and how risks are managed, showing that technology plays a direct role in protecting, or sometimes threatening, human rights.

The overarching goal of Envirotech is to protect and restore the environment, decrease pollution, and utilise natural resources more efficiently. By achieving these aims, Envirotech endeavours to reduce human impact on the environment and help restore ecological balance. Environmental technologies can be grouped into key areas, including clean energy, pollution control, water and sanitation, climate resilience, and sustainable agriculture.

1. *Clean Energy Technologies:* These solutions focus on generating power from renewable sources, thereby reducing dependence on fossil fuels and carbon emissions. Examples include solar panels, wind turbines, hydropower systems, and geothermal plants. This category also extends to energy management systems such as LED lighting, high-efficiency appliances, smart grids, and advanced insulation, all aimed at reducing overall energy consumption.
2. *Pollution Reduction and Waste Management:* These include technologies designed to remove harmful pollutants from the atmosphere and water bodies. Specific examples include air scrubbers and catalytic converters, which purify air, and wastewater treatment plants, which clean polluted water.
3. *Water and Sanitation Technologies:* Critical for protecting human health and the environment, these technologies ensure access to clean water and proper waste disposal. Examples include membrane filtration, decentralised treatment plants, safe drinking water systems, and infrastructure for wastewater recovery or effluent disposal.
4. *Climate Resilience and Mitigation Technologies:* These technologies help societies adapt to the increasing frequency and intensity of extreme climate events and reduce greenhouse gas emissions. Flood defences, drought-resistant crops, and early warning systems are crucial for adaptation, potentially saving lives. On the mitigation side, technologies such as carbon capture and storage, reforestation tools, and improved green infrastructure help reduce emissions and enhance environmental resilience.
5. *Sustainable Agriculture Technologies:* Innovations in this field, such as precision farming, vertical agriculture, and organic pest control, help increase productivity with lower chemical inputs while conserving water and soil, contributing to more sustainable food systems.

Research Project, Local Case Exploration: Pick an SEA country and research a tech project (e.g., AI, renewables). Describe its impacts in a 300-word report or poster. Reflect: How could your community adopt it, and what safeguards protect vulnerable groups?

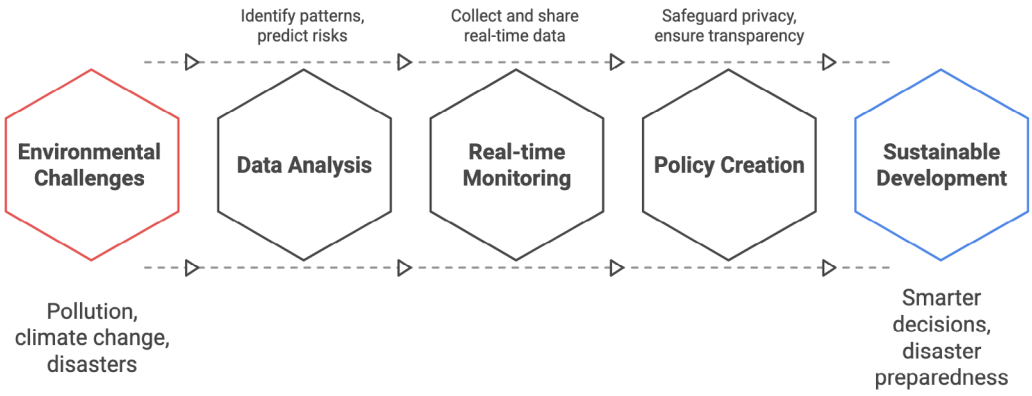
ASEAN has promoted the adoption of Envirotech under the framework of the ASEAN Digital Masterplan 2025 and green economy strategies. The ASEAN Digital Community 2045 emphasises balancing technological growth with sustainability, addressing challenges such as the projected rise in e-waste to 75 million tonnes by 2030, and ensuring equitable access and local capacity-building. How can SEA implement these technologies to benefit all communities while minimising environmental harm? The next section discusses examples of emerging technologies applications in the environmental context.

6.3.1 AI and IoT for Environmental Monitoring

Artificial Intelligence (AI) and the Internet of Things (IoT) are transforming how Southeast Asia monitors and protects its environment. These technologies help governments, scientists, and communities respond more quickly and effectively to challenges such as pollution, climate change, natural disasters, and biodiversity loss.

AI works by analysing enormous amounts of data collected from satellites, drones, and ground sensors. It uses this data to identify patterns, predict future risks, and issue early warnings about environmental events such as floods, droughts, and declining air quality. IoT, on the other hand, is a network of interconnected devices, from air quality sensors to water level monitors, that continuously collect and share real-time data about the environment. As illustrated in Figure 6.4, AI and IoT enables real-time analysis of sensor data, enabling early warnings, better decision-making, and more effective environmental protection.

Figure 6.4: AI and IoT for Environmental Protection



Across Southeast Asia, these technologies are already making a difference. In the Philippines, AI-powered flood prediction systems in Manila analyse weather data, rainfall patterns, and drainage capacity to issue early warnings. This has helped protect residents from typhoons and rising sea levels, reducing deaths and property damage. IoT sensor networks in Singapore and Indonesia are another example. These systems track fine particulate matter or pollution caused by transboundary haze from peatland fires and alert residents via mobile apps. In Thailand, Bangkok's AI Nowcast predicts rainfall up to three hours before it occurs, giving communities more time to prepare and reducing flood-related damage. Along the coasts of Indonesia and Malaysia, AI-powered acoustic systems detect illegal fishing activity, protecting marine biodiversity and supporting the livelihoods of indigenous fishing communities that rely on healthy fish stocks.

Despite their promise, AI and IoT come with ethical challenges. The extensive data they collect, especially about people's locations, habits, or communications, could be misused. For instance, the use of AI-enabled drones and IoT sensors for environmental monitoring can raise human rights concerns, particularly related to privacy and the surveillance of environmental defenders. These risks are addressed through Human Rights and Environmental Due Diligence (HREDD), which requires companies to identify and prevent potential harms before deploying new technologies. For example, in a drone-based forest monitoring project, a company must assess who may be affected, such as Indigenous communities or local activists, and how data collection could be misused for tracking or intimidation. To reduce these risks, HREDD requires limiting data collection to environmental purposes, avoiding facial recognition, consulting affected communities, and restricting access to sensitive data. Ongoing monitoring and accessible complaint mechanisms help ensure that environmental technologies protect human rights rather than undermine them.

Case study: AI, Forests and Rights in Indonesia

In Indonesia, vast rainforests covering millions of hectares face ongoing threats from illegal logging and the expansion of palm oil plantations. AI-driven deforestation monitoring now plays a crucial role in protecting both the environment and human rights. Projects such as Planet Indonesia's bioacoustics system use artificial intelligence to analyse forest soundscapes and detect chainsaw noises or human activity in real time across Kalimantan and Sumatra. Satellite imagery from platforms like Farmonaut and drone-based LiDAR from FlyPix AI further enhances detection.

These technologies help reduce forest loss in monitored areas, preserve biodiversity hotspots that absorb carbon, and mitigate the impacts of climate change, which heavily affect Indigenous communities. They also strengthen the right to self-determination by giving Indigenous groups access to monitoring data through mobile apps, allowing them to enforce land rights and challenge encroachment without relying on external actors. These initiatives have helped to protect forests and support the creation of community-led patrols that safeguard cultural heritage.

However, challenges remain: high implementation costs exclude many remote villages, and drone surveillance raises privacy concerns. The key lesson is that while AI can protect the right to a healthy environment and reduce hazards like haze pollution, it must ensure equitable access and responsible data use so that it empowers, rather than alienates, the communities it aims to protect.

Reflection and Discussion:

If a drone catches loggers while also spying on villagers, how does that affect villagers' trust in technology? What safeguards could protect their privacy?

6.3.2 Renewable Energy Innovations

Renewable energy is energy that comes from natural sources such as sunlight, wind, water, and ocean tides, which can be replenished over time. Unlike fossil fuels, which release greenhouse gases and damage the environment, renewable energy is clean and sustainable, making it one of the most important tools for fighting climate change and building a greener future. In Southeast Asia, countries are combining both traditional technologies and digital innovations to transform how energy is produced, distributed, and used, creating a story of transition toward a more sustainable region.

Imagine villages once dependent on diesel generators are now powered by the sun. Across ASEAN, solar farms are expanding rapidly, making clean energy more affordable for homes and businesses. In Malaysia, ocean currents are being harnessed through tidal energy projects along the coast of Sabah. These projects generate electricity without occupying large areas of land, helping avoid conflicts with indigenous communities and protecting their ancestral land rights.

Hydropower is another key part of the story. In Sarawak, large hydropower plants provide nearly one-third of new clean energy demand, delivering electricity to millions of people. Yet, this technology requires careful planning to ensure that dams do not displace communities or disrupt local ecosystems. New digital technologies make these systems even smarter. AI-powered smart grids manage how electricity flows across countries, predicting demand, balancing supply, and reducing energy waste. These intelligent networks also support renewable sources like solar and wind, which can vary depending on weather conditions, ensuring that energy remains stable and reliable.

This transformation is not just about technology; it is also about people and opportunities. The shift to renewables is expected to create millions of green jobs and supporting inclusive development. But as the region embraces this clean energy future, a key question remains: How can Southeast Asia expand renewable energy while ensuring that vulnerable communities are protected from disruption and included in the benefits of this transition?

Case Study: Powering Rights: Solar Energy and Social Change in Vietnam

Vietnam's rapid solar energy expansion shows how renewable technology can advance environmental sustainability, health, and social equity, while also raising complex human rights challenges. In just a decade, the country increased its solar capacity from 4 megawatts to more than 18 gigawatts, driven by government Feed-in Tariffs and AI-optimised smart grids that deliver stable power to remote areas such as Trà Vinh province.

This shift reduces dependence on fossil fuels, cuts millions of tonnes of greenhouse gas emissions, and replaces polluting diesel generators, leading to a 20% drop in respiratory illnesses among children and the elderly in off-grid communities. The benefits extend beyond health. Women-led cooperatives managing local microgrids create new income opportunities and promote gender equity, in line with the principles outlined in the Paris Agreement.

However, the solar boom also presents challenges. The construction of large-scale solar farms has displaced about 500 farming families, threatening their right to self-determination and food security. Poorly managed battery waste risks contaminating water sources, and retroactive price changes for solar projects have placed financial strain on small investors.

The case illustrates how renewable energy strengthens the right to a healthy environment and supports sustainable development, but it must be accompanied by fair compensation, inclusive decision-making, and responsible waste management to avoid reinforcing inequalities in vulnerable rural communities.

Reflection and Discussion:

Examine Vietnam's solar boom: How do the solar farms impact rights (e.g., health for kids) and challenges (e.g., land use). Present the findings, and propose adaptations for your community.

6.3.3 Blockchain for Sustainable Supply Chains

Blockchain is a type of digital record-keeping system that securely and transparently stores information. You can think of it as a shared online notebook that everyone can see, but no one can change or erase once something is written in it. Every new piece of information is stored as a "block" and linked to the one before it, forming a "chain." Because the information is permanent and verified, it builds trust between people, businesses, and governments.

One of the most important uses of blockchain in Southeast Asia is tracking how products move from their source to the final consumer, a process known as the supply chain. A supply chain is simply the journey a product takes from where it is produced (like a farm, forest, or mine) to where it is sold and used. Many human rights and environmental problems happen along this journey, such as illegal logging, land grabbing, or unfair treatment of workers. Blockchain helps address these problems by recording every step of the journey in a transparent way that anyone can check.

For example, in Malaysia, blockchain is used to trace palm oil from plantations in Sabah to global markets, verify sustainability claims, and enforce No Deforestation, No Peat, No Exploitation (NDPE) policies. The platform has achieved almost 100% traceability, meaning companies and consumers can see exactly where the palm oil comes from and whether it was produced without harming forests or violating workers' rights.

This system also helps small-scale farmers get fair access to global markets, improving their incomes and livelihoods. Using blockchain with satellite data to map supply chains in real time also helps reduce biodiversity loss, prevent deforestation, and protect indigenous communities whose lives and cultures are closely connected to their ancestral lands. Companies are also combining blockchain with AI and location data to ensure palm oil is sourced responsibly and without exploitation. These innovations make companies more accountable for their actions and support environmental justice by linking profit to ethical behaviour. They also strengthen human rights by protecting communities, workers, and the environment from abuse.

Reflection and Discussion:

In your social media feed, do ads for "sustainable" items make you question their claims? Explore how blockchain could verify these in real life, and debate if it empowers consumers or just benefits big companies.

6.3.4 Geoengineering and Climate Adaptation

Imagine Earth as a shared home, and in Southeast Asia, this home is already under stress. Temperatures are rising, rainfall is unpredictable, storms are stronger, and sea levels are creeping higher. Governments know that cutting greenhouse gas emissions is essential, but they are also exploring tools to actively shape the climate itself.

Geoengineering refers to large-scale, intentional interventions in Earth systems aimed at moderating climate change, particularly global warming. These interventions are typically categorised into Solar Radiation Management (SRM), which seeks to reflect a portion of incoming solar radiation to cool the planet, and Carbon Dioxide Removal (CDR), which aims to extract greenhouse gases from the atmosphere and store them long term. As a form of envirotech, geoengineering is characterised by: system-level intervention in atmospheric or oceanic processes; heavy reliance on advanced modelling, aerospace, and chemical technologies; and high levels of scientific uncertainty and potential irreversibility. While geoengineering is often framed as a technological response to the climate emergency, it raises ethical, political, and governance challenges. There is growing concern that certain geoengineering responses to climate change, particularly large-scale SRM may pose risks that rival or exceed their potential benefits. Techniques such as injecting sulphur-based aerosols into the stratosphere could temporarily lower global temperatures, but they carry significant uncertainties and risks, including acid deposition, disruption of precipitation patterns, and damage to the ozone layer. Moreover, geoengineering raises the problem of moral hazard, whereby the prospect of technological climate control may weaken incentives for greenhouse gas mitigation. For these reasons, large-scale geoengineering projects have not been endorsed at the international level and remain largely confined to modelling studies and governance debates rather than deployment.

In contrast, climate adaptation technologies focus on enhancing the capacity of human and natural systems to cope with the impacts of climate change. These technologies operate at local to regional scales and are designed to work with, rather than override, existing ecological and social systems. Examples of adaptation-oriented envirotech include: early warning systems for floods, cyclones, and heatwaves; climate-resilient infrastructure and urban design; nature-based solutions such as mangrove restoration and wetland conservation; and precision agriculture and water management technologies. Adaptation-focused envirotech is typically lower risk, more reversible, and better aligned with principles of climate justice and human-centred design. Importantly, such technologies often deliver co-benefits, including biodiversity conservation, livelihood protection, and improved public health.

Case Study: Climate Adaptation Technologies in ASEAN

Precision Agriculture: In countries such as Vietnam and Thailand, farmers are increasingly using digital decision-support tools and sensor-based monitoring to implement Alternate Wetting and Drying (AWD) in rice paddies. This climate-smart practice reduces water use and methane emissions while maintaining yields, even under rising temperature stress.

Nature-Based Infrastructure: The Philippines and Indonesia are regional leaders in blue carbon initiatives, combining satellite data, drone-based monitoring, and community-led restoration to rehabilitate mangrove forests. These ecosystems function as natural bioshields against sea-level rise and intensified typhoons, while also contributing to carbon sequestration.

Urban Cooling: Cities such as Singapore and Bangkok are deploying cool roofs, vertical greenery, and digitally supported energy-efficiency measures to mitigate the Urban Heat Island effect, reducing heat exposure and supporting public health during extreme heat events.

6.3.5 Biotechnology in Agriculture

Biotechnology is the use of scientific techniques involving living organisms, such as plants, microorganisms or genetic material, to address real world challenges. In agriculture, it includes a range of tools aimed at improving crop resilience, productivity, and sustainability. This approach is becoming increasingly important in Southeast Asia, where farmers face growing pressures from climate change, water scarcity, and soil degradation.

In Thailand, researchers have applied CRISPR-based gene-editing techniques to improve traits in the KDML105 (jasmine rice) variety, including enhanced tolerance to drought-related stress. While these innovations remain largely at the research and pilot stages, they demonstrate the potential of biotechnology to support future food security amid increasingly unpredictable rainfall patterns. In Malaysia, biotechnology-assisted breeding, using genomic tools and tissue culture, has been employed to improve the climate resilience of oil palm, including efforts to maintain productivity during periods of water stress. These developments aim to support the livelihoods of farmers and rural communities that depend heavily on palm oil production. Indonesia has pursued a complementary approach by adopting aerobic rice systems, which require substantially less water than conventional flooded paddy cultivation while maintaining stable yields in drought-prone areas. Although not a form of biotechnology, this climate-smart agricultural practice is often supported by improved crop varieties and helps reduce pressure on water-stressed ecosystems.

Another important area where biotechnology is being applied to reduce greenhouse gas emissions is livestock management. Cattle produce methane during digestion, and methane is a significantly more powerful warming gas than carbon dioxide. Recent research indicates that adding certain feed supplements, such as red seaweed, to animal diets can substantially reduce rumen methane production. These dietary interventions have been shown to lower emissions per animal by approximately 30–80% under experimental and pilot conditions, offering a promising pathway toward more climate-friendly livestock systems.

Together, these technological and agronomic innovations extend beyond yield improvement. They contribute to food security, strengthen rural livelihoods, and support the realisation of the right to food by enabling farming communities to adapt to environmental change while maintaining continuity with local agricultural practices.

Reflection and Discussion:

How do genetically modified foods in your supermarket (e.g., drought-resistant rice or veggies) affect your right to healthy, sustainable food? Discuss a meal where you considered food origins and how biotech might help or harm small farmers in your area.

Case Study: Carbon Capture and Community Rights in Singapore

Singapore's carbon capture and storage (CCS) pilot project illustrates how technological innovation can reduce emissions in a highly urbanised environment while raising important questions about rights and governance. Implemented at Jurong Island and several waste-to-energy plants, the initiative involves several companies. It captures tonnes of CO_2 annually from industrial sources, storing it underground or repurposing it for other uses.

Artificial intelligence plays a key role in optimising capture efficiency. The project reduces greenhouse gas emissions by about 15 percent in targeted sectors, helping to address sea-level rise and urban heat while directly supporting the right to a healthy environment by improving air quality for 5.7 million residents. The initiative supports Singapore's net-zero ambitions, creates new employment opportunities in green engineering, and improves public health by reducing pollution-related health risks.

However, it also faces significant challenges. High operational costs could place pressure on public resources. Limited public participation in planning processes risks excluding communities from decisions about storage safety, particularly concerning potential leaks that could affect water quality. In addition, the high energy demand of carbon capture facilities may offset environmental benefits if the energy comes from non-renewable sources.

A larger problem is that many countries in the region rely on yet to be discovered CCS technology to meet their 20250 goals of reduction GHGs. Fossil fuel industries are claiming that they can continue to drill for fossil fuels because they will find a way to capture it. The promise of these technologies justifies the unsustainable use of fossil fuels and delays real action to reduce GHG emmisssions..

This case shows that while CCS strengthens the right to health and advances sustainability goals, it must be accompanied by transparent governance, meaningful public involvement, and respect for procedural rights such as access to information and justice to ensure that technological progress aligns with community needs and values.

Reflection and Discussion:

Imagine you live near Jurong Island and learn that carbon capture facilities are operating close to your community. You are told the project improves air quality and supports climate goals, but little information is shared about long-term storage safety or possible risks. What information would you expect the government and companies to provide, and how does access to information support the right to a healthy environment?

6.4 ASEAN Approaches to Emerging Technologies and Environment

Southeast Asia is increasingly shaping its legal and policy approaches to emerging technologies by grounding them in global human rights and environmental standards while adapting them to the region's specific realities. Guided by principles from instruments such as the Paris Agreement, the Aarhus Convention, and the UN Guiding Principles on Business and Human Rights (UNGPs), ASEAN and its member states are developing frameworks that aim to ensure technology serves the public good rather than undermines fundamental rights. These efforts involve translating international norms into regional and national policies that reflect local priorities. Ultimately, a robust legal and policy framework ensures that innovation contributes to sustainable development, respects human rights, and empowers communities to participate in shaping the environmental future of the region

ASEAN uses technology extensively for climate governance, driving transparency and transformation toward its climate vision 2050. Technological application focuses on strengthening the science and information base through tools like Digital Transformation (DX), developing advanced MRV systems (such as a planned knowledge centre hub on MRV), and strengthening the modelling capacity for long-term projections to inform ambitious Nationally Determined Contributions (NDCs) and long-term strategies. Furthermore, technology accelerates transformation through the diffusion of low- and zero-carbon technologies, expansion of Renewable Energy (RE), and accelerating regional power interconnectivity. This governance framework directly relates to principles of human rights by mitigating the severe impacts of climate change on the most vulnerable sectors of society and ensuring solutions enhance societal well-being. Mitigation efforts, such as the switch to clean energy, generate multiple co-benefits like improving electricity access, creating local green jobs, and reducing air pollution, while ASEAN explicitly integrates strategies for a just transition to reskill the workforce and assist in smooth reemployment in climate-friendly industries while discussions on an ASEAN Declaration on Environmental Rights signal a growing recognition of the need to codify environmental rights and embed them into regional legal frameworks.

On October 28, 2025, ASEAN adopted the "ASEAN Declaration on the Right to a Safe, Clean, Healthy and Sustainable Environment" at the ASEAN Summit in Kuala Lumpur, Malaysia. This landmark document explicitly affirms the universal human right to such an environment, emphasizing its links to peace, security, sustainable development, and other human rights. Key provisions include commitments to substantive elements (e.g., protection from environmental harm) and procedural rights (e.g., access to information, public participation, and justice), with special attention to vulnerable groups like children, women, and Indigenous peoples. It urges member states to integrate these principles into national laws and policies, including technology deployment. However, critiques from civil society organizations, such as Greenpeace and human rights experts, highlight its non-binding nature, aspirational language that lacks enforceable mechanisms, omission of corporate responsibilities to uphold environmental rights, failure to address root causes like extractive industries, and insufficient protections for environmental defenders facing threats. These limitations underscore the need for stronger implementation to translate the declaration into actionable rights-based tech governance.

Beyond these initiatives, environmental protection, conservation, and sustainability also form a pillar of the ASEAN Socio-Cultural Community (ASCC) Blueprint 2025 under the characteristic of Sustainable. The ASCC is committed to cooperative activities that are people-oriented, people-centred, environmentally friendly, and geared towards the promotion of sustainable development. The blueprint recognizes its importance for modernization and dynamism, seeking to harness the use of information and communication technologies (ICT) for greater access, lifelong learning, and competitiveness, promoting the adoption of environmentally-sound technologies for resource efficiency, encouraging the utilization of renewable energy and green technologies to enhance resilience, and strengthening institutional capacity with advanced technological and managerial skills to address emerging challenges like climate change

While the **ASEAN Plan of Action for Energy Cooperation (APAEC) 2016–2025, Phase II**, is framed around the 4th Industrial Revolution (4IR), critics argue that the plan masks a continued commitment to carbon-intensive infrastructure. By integrating artificial intelligence and big data into the fossil fuel sector, the plan attempts to optimise coal and gas rather than phasing them out. While the industry promotes Clean Coal Technology (CCT) and Carbon Capture, Utilisation, and Storage (CCUS) as viable pathways, environmental scientists frequently problematize these terms as "greenwashing." They argue that "clean coal" is a technical misnomer; even with carbon capture, the upstream environmental costs—such as methane leakage from mining and the toxic footprint of coal ash—remain unaddressed, making the "clean" claim a significant fabrication. The APAEC theme of "Enhancing Energy Connectivity" to achieve **UN SDG7** (affordable and reliable energy) is often used to justify expanding coal and gas under the guise of affordability and energy security. However, environmentalists disagree with this logic, asserting that the plan fails to address the "carbon lock-in" effect. By investing billions into new gas pipelines and coal upgrades, ASEAN risks stranding assets and falling behind in the global energy transition. Critics contend that for a region so vulnerable to sea-level rise and extreme weather, the "affordability" of coal is a short-sighted illusion that ignores the massive "externalised costs" of climate-related healthcare, crop failure, and disaster relief.

In contrast to the fossil-centric focus of the APAEC, the ASEAN Action Plan on Environmentally Sustainable Cities (ESC) offers a more genuine response to the climate crisis. By prioritising green infrastructure and digital air quality monitoring, the ESC framework links technological innovation to the immediate health and rights of urban citizens. Environmentalists argue that the APAEC should be re-aligned with these principles, moving away from "pro-fossil" innovation toward a decentralised, decarbonised energy system. The central conflict remains: while ASEAN's energy needs are growing rapidly, using that growth to justify coal and gas expansion undermines the very energy security and "sustainability for all" that the region claims to uphold.

To bolster enforcement and public participation, citizens have utilised Environmental Public Interest Litigation (EPIL) as a mechanism to advance environmental rights. EPIL allows citizens, NGOs, and communities to file lawsuits against polluters or governments for environmental harms, thereby supporting procedural rights under frameworks such as the Aarhus Convention and the new ASEAN Declaration. Notable examples include the Philippines' Writ of Kalikasan, an environmental writ enabling rapid judicial intervention for ecosystem threats (e.g., in the Manila Bay rehabilitation case, 2008–ongoing); Indonesia's public suits under the 2009 Environmental Protection and Management Law, which have challenged deforestation and mining; and Thailand's administrative court cases, such as the 2022 coalmine lawsuit highlighting air pollution impacts. Technologies play a key role in EPIL by providing evidence, such as satellite imagery for deforestation claims or AI-analyzed data for pollution monitoring, empowering marginalized groups to hold actors accountable. However, challenges persist, including high litigation costs, limited access to environmental information (e.g., restricted Environmental Impact Assessments), weak enforcement of judgments, and low legal awareness, as noted in reports like EarthRights International's 2024 briefing. Addressing these through capacity-building and tech-enabled data transparency is essential for EPIL to effectively bridge governance gaps.

ASEAN's approach to disaster risk management has gradually shifted from mainly reacting to emergencies toward building long-term resilience using digital technologies. This shift is reflected in the **ASEAN Agreement on Disaster Management and Emergency Response (AADMER) Work Programme 2021–2025**, which emphasizes the use of information and communication technologies (ICT) to improve how countries prepare for and respond to disasters. Rather than focusing only on individual tools, ASEAN promotes a more coordinated digital system that allows data to inform early warnings, preparedness, and decision-making. A key part of this approach is the **Digital Disaster Risk Reduction Maturity Model (DDRRMM)**. This framework encourages ASEAN member states to move beyond simply adopting new technologies and instead build the capacity to use digital data effectively in planning and response. The goal is to ensure that information from different

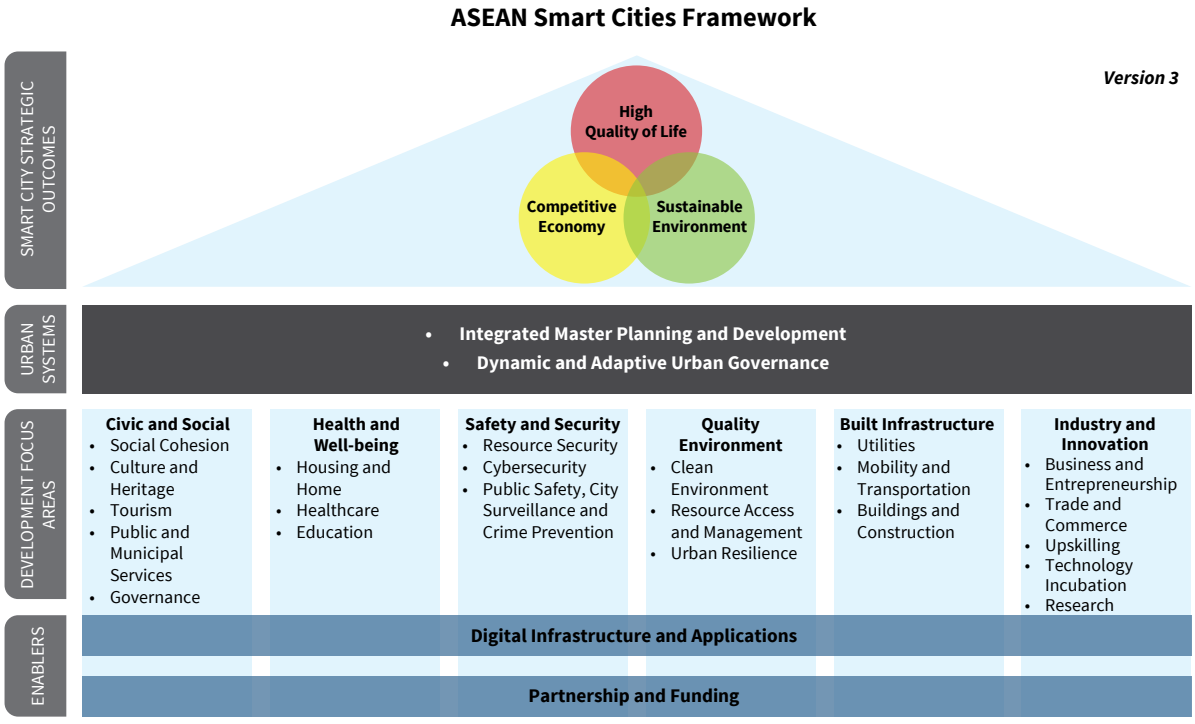
sources supports timely action, improves coordination, and influences how governments and communities prepare for disasters.

At the technical level, ASEAN relies heavily on **Geographic Information Systems (GIS)** and **satellite-based Earth observation** to monitor hazards and assess risk. These tools are increasingly combined with **participatory mapping**, which allows local communities to contribute information and improve the accuracy of risk assessments. While the use of **artificial intelligence (AI)** and **big data** is still limited, early examples—such as predictive models used during the Philippines' response to Typhoon Haima—show how data analysis can support faster and more effective decision-making. In addition, some ASEAN countries are using **drones (UAVs)** and robotics to assess damage in hard-to-reach areas, especially when roads and communication networks are disrupted.

Despite these advances, there is still a gap between using digital tools for monitoring and fully integrating new technologies into disaster response logistics. Technologies such as **blockchain** and **digital cash transfers** could improve transparency and efficiency in humanitarian aid, but they are not yet widely used by regional institutions like the **ASEAN Coordinating Centre for Humanitarian Assistance (AHA Centre)**. Similarly, innovations such as **3D printing** could help produce essential supplies more quickly during emergencies but remain largely experimental. The main challenge for ASEAN moving forward is to close this gap by turning promising technologies into shared, standardized systems that strengthen regional disaster response beyond 2025.

One of the most significant efforts is the ASEAN Smart Cities Network (ASCN) 2018, a collaborative platform in which 26 pilot cities from 10 ASEAN states work together to develop smart and sustainable cities. The ASEAN Smart Cities Framework, a non-binding guide, emphasises using technology to improve the quality of life while acknowledging the need to incorporate human rights through a focus on inclusivity, equity, and security. For instance, the city's smart public transport system includes real-time bus tracking and mobile applications designed for persons with disabilities, ensuring equitable access to mobility. (See Figure 6.2).

Figure 6.2: ASEAN Smart Cities Framework 2018 https://asean.org/wp-content/uploads/2019/02/ASCN-ASEAN-Smart-Cities-Framework.pdf



The significant reliance on data-intensive infrastructure, however, directly interacts with digital rights by highlighting severe governance challenges: ASEAN currently lacks a comprehensive, unified data regulation, unlike the EU-GDPR, resulting in regulatory fragmentation regarding basic definitions of personal data and data subjects' rights among ASEAN Member States (AMS). To address ASEAN's data governance strategy, focused on realising the Digital Economy Framework Agreement (DEFA), ASEAN aims to achieve Data Free Flow with Trust (DFFT) by balancing data flows with the necessary protections for privacy, security, and intellectual property.

You Are Here: Why Data Governance Matters to You

When environmental data is shared quickly and responsibly, people receive earlier warnings and better protection. When data is delayed, misused, or mistrusted, communities are left exposed. Trust in how data is collected and shared directly affects whether environmental technologies actually keep people safe.

However, governance is hampered by a lack of harmonisation of laws across its member states, including inconsistent definitions of personal data and differing legal grounds for processing. Recommendation to establish the ASEAN Data Governance Hub for transparency and mandating minimum standards for Personal Data Protection (PDP) aligned with OECD Privacy Guidelines. This extensively relates to human rights through the core focus on data privacy and protection, detailing differences in the rights afforded to data subjects (such as the rights to access, rectify, and delete data), and stressing the need for robust safeguards against governmental access to personal data to protect privacy and human rights and freedoms, adhering to principles of legal basis and transparency.

Reflection and Discussion:

Imagine you live in a coastal town in Southeast Asia. Heavy rain upstream in another country often causes floods in your area. To protect communities, governments use environmental technologies such as satellite images, river sensors, and AI systems to predict floods and send early warnings. For these systems to work, data must flow quickly across borders. If one country delays or withholds information, the warning comes too late, and people may lose their homes or even their lives. Now imagine that drones are also used to monitor forests and rivers near your community. While these technologies can help protect the environment, people may worry about who is collecting the data and how it will be used. Will the drone footage only track pollution and deforestation, or will it also record daily activities, identify protest leaders, or monitor environmental defenders? If there are no clear rules on data protection, trust in these technologies quickly disappears.

- *In the flood situation, what could happen if countries do not share environmental data quickly?*
- *Why might communities feel uncomfortable with drones or sensors if there are no clear rules on how data is used?*
- *Do you think protecting privacy could ever slow down environmental protection? How does Data Free Flow with Trust (DFFT) try to balance both concerns?*

6.5 Conclusion

This chapter showed how environmental challenges in Southeast Asia, such as climate change, pollution, deforestation, and disasters, are not just environmental issues, but human rights issues that affect people's health, livelihoods, and dignity. These crises are felt most strongly by vulnerable groups, including Indigenous peoples, women, and future generations. It also explained the rights frameworks that guide fair environmental decision-making, including the right to a healthy environment, climate justice under the Paris Agreement, corporate accountability, and procedural rights like participation and free, prior, and informed consent (FPIC). These frameworks help answer who is responsible and how people should be protected.

Finally, the chapter explored environmental technologies as the tools that turn these principles into reality. Technologies such as AI monitoring, renewable energy, and climate data systems can protect the environment, but only when they are designed and used with strong human rights safeguards. Most importantly, this chapter reminds you that you are not just a learner, but a future decision-maker. The way you question "green" solutions, use technology, and demand accountability will help shape whether environmental protection in Southeast Asia is fair, inclusive, and just.

Key Takeaways

1. Southeast Asia's environmental challenges, deforestation, pollution, biodiversity loss, and climate vulnerabilities like rising seas and typhoons, are more than ecological crises; they're human rights threats that undermine food security, health, housing, and livelihoods for millions, especially in vulnerable communities.
2. The right to a safe, clean, healthy, and sustainable environment (RtHE) encompasses substantive elements (clean air, water, food, ecosystems) and procedural rights (information, participation, remedies), forming the foundation for rights-based responses to degradation and climate change.
3. Environmental technologies (envirotech) span clean energy, pollution reduction, waste management, and climate adaptation/mitigation, offering tools like solar grids and AI monitoring to address regional issues, but their deployment must align with human rights to avoid harms like displacement or inequality.
4. Geoengineering and other emerging tech pose significant risks, from unintended ecological disruptions to violations of self-determination and FPIC for Indigenous peoples, requiring rigorous due diligence and equity-focused governance.
5. Climate justice demands fair distribution of envirotech benefits and burdens, prioritizing marginalized groups like women and future generations, as seen in frameworks like the Paris Agreement and REDD+ programs that can either empower or exploit communities.
6. ASEAN's approaches show promise in integrating innovation with rights, but gaps in enforcement, data access, and participation must be bridged to ensure inclusive, sustainable progress.
7. Envirotech's potential in Southeast Asia is immense, but only if we choose justice over exploitation, ensuring innovations respect dignity, protect ecosystems, and empower all to build a resilient future.

Issues to Think About

1. If a "green" project like a wind farm or dam were proposed near your home, potentially displacing families or altering local ecosystems, do you believe communities should have veto power through FPIC? Why or why not, and how could you personally advocate for it?
2. When you discard an old phone or gadget, contributing to e-waste that pollutes communities in Southeast Asia, how does this connect to your right to a healthy environment? What small changes could you make to demand better corporate accountability?
3. Imagine a geoengineering experiment to combat haze or floods in your region goes wrong, affecting weather and agriculture for years—should governments owe compensation to impacted people? Relate this to intergenerational equity and who should decide on such tech.
4. In your daily life, do apps for air quality or waste tracking help you feel more empowered against pollution? How might unequal access to these tools deepen climate injustice for rural or low-income groups, and what actions could you take to promote fair distribution?
5. Should businesses deploying envirotech, like mining for renewable energy materials, be legally required to conduct human rights and environmental due diligence (HREDD)? Pick a real example from Southeast Asia and explain how it could prevent harms.
6. Ten years from now, do you want to live in a Southeast Asia where envirotech has reduced climate threats but at the cost of Indigenous rights, or one where rights-based innovation ensures equity for all? Which path are you willing to support through your choices?

Further Readings

ASEAN Parliamentarians for Human Rights. (2025). *ASEAN vision 2045 falling short on human rights and democratic reform*. https://aseanmp.org/publications/post/asean-vision-2045-falling-short-on-human-rights-and-democratic-reform-says-aphr/

ASEAN. (2021). *Sixth ASEAN state of the environment report*. https://asean.org/wp-content/uploads/2023/09/Sixth-ASEAN-State-of-the-Environment-Report-SOER6_20240517_COMPRESSED.pdf

Business & Human Rights Resource Centre. (2024). *Human rights in Southeast Asia's renewable energy transition: Analysing company policies*. https://www.business-humanrights.org/en/from-us/briefings/southeast-asia-renewable-energy-analysis-2024/

Chew, Y. I., Ooi, S. Y., Ling, Y. H., & Wong, K. S. (2022). A review of forest fire combating efforts, challenges and future directions in Peninsular Malaysia, Sabah, and Sarawak. *Forests*, *13*(9), 1405. https://doi.org/10.3390/f13091405.

EarthRights International. (2023). *Enhancing the role of environmental public interest litigation to advance environmental rights in Southeast Asia*. EarthRights Briefing Report. https://earthrights.org/wp-content/uploads/2024/01/Enhancing-the-Role-of-Environmental-Public-Interest-Litigation-to-Advance-Environmental-Rights-in-Southeast-Asia.pdf

Feroz, A. K., Zo, H., & Chiravuri, A. (2021). Digital transformation and environmental sustainability: A review and research agenda. *Sustainability*, *13*(3), 1530. https://doi.org/10.3390/su13031530

Human Rights Watch. (2024). *ASEAN environmental rights declaration needs transparency*. https://www.hrw.org/news/2024/06/30/asean-environmental-rights-declaration-needs-transparency

Kim, Dayoon, Das, P., & Canales, N., (2025). Advancing the right to a healthy environment in Southeast Asia. *SEI Publications*. https://www.sei.org/publications/right-to-healthy-environment-southeast-asia/

Knox, J., & Morgera, E. (2022). *Human rights and the environment: The interdependence of human rights and a healthy environment in the context of national legislation of natural resources* (FAO Legal Paper 109). Food and Agriculture Organization of the United Nations. https://openknowledge.fao.org/server/api/core/bitstreams/e3bd01ca-c033-44dd-9262-c29c7c75e166/content

Kshetri, N., Rojas, D. C. T., Besada, H., & Moros Ochoa, M. A. (2020). Big Data as a tool to monitor and deter environmental offenders in the Global South: A multiple case study. *Sustainability*, *12*(24), 10436. https://doi.org/10.3390/su122410436

Raoul Wallenberg Institute of Human Rights and Humanitarian Law. (2024). *Prosperous and green in the Anthropocene: The Human Right to a Healthy Environment in Southeast Asia*.

Sharom, A., Petcharamesree, S., and Dutta, K., (Eds). (2024) Human Rights, The Environment and Climate Change (Volume 5). https://www.scribd.com/document/901657541/Human-Rights-the-Environment-and-Climate-Change-2024

Stockholm Environment Institute. (2024). *The ASEAN declaration on environmental rights: Whose rights and what rights?*https://www.sei.org/perspectives/asean-declaration-environmental-rights/

The ASEAN Secretariat (2025). *ASEAN declaration on the right to safe, clean, healthy and sustainable environment*. https://asean.org/wp-content/uploads/2025/10/5.-ASEAN-Declaration-on-the-Right-to-a-Clean-Safe-Healthy-and-Suitable-Environment.pdf

United Nations Conference on Trade and Development. (2025). *World investment report 2025: International investment in the digital economy*. https://unctad.org/publication/world-investment-report-2025

Chapter 7:

Bridging the Digital Divide and Ensuring Digital Inclusion

Reader's Guide

Welcome to the chapter that tackles the big question: why does the digital divide persist in Southeast Asia, leaving so many behind in our tech-driven world? Is it just about internet access, or deeper issues like affordability, skills, and rights? Here, you will see how this gap widens inequalities in education, healthcare, and civic participation, especially for vulnerable groups such as rural communities, women, and MSMEs. You will also discover a Human Rights-Based Approach (HRBA) that champions equality, participation, and accountability, along with practical ways such as multi-stakeholder collaborations and digital finance to foster inclusion. By the end, you'll be equipped to spot digital injustices and advocate for a more equitable tech landscape in the ASEAN region.

In this chapter, you will:

- Understand the digital divide in Southeast Asia, its regional stats, and six key dimensions: affordability, availability, digital education, digital security, environment, and resilience.
- Analyse structural gaps that reinforce inequality, from economic hurdles for MSMEs to political-legal controls and social-cultural biases.
- Apply a Human Rights-Based Approach (HRBA) to digital inclusion, aligning it with core principles and four spheres of digital rights.
- Discover alternative approaches to bridge the divide.
- Let's close that gap and build a digital Southeast Asia where everyone thrives.

Key Terms

- **Digital Divide**: The gap between individuals, communities, or nations in accessing, using, or benefiting from digital technologies, influenced by socio-economic, geographic, and demographic factors.
- **Digital Literacy**: The ability to find, evaluate, and communicate information effectively through a knowledge of digital rights using digital tools.
- **Human Rights-Based Approach (HRBA)**: A framework for ensuring developmental activities, policy, and other programs are undertaken using international human rights instruments as the foundation. The objective is for individuals to claim their rights while holding governments and organizations accountable, in this case in the digital realm.
- **Data Representation (Digital Rights)**: One of the four spheres of digital rights focusing on an individual's rights related to personal data in the digital realm, including data privacy, freedom from digital surveillance, and non-discrimination in data use.
- **Inclusive Digital Economy**: An economic model that expands financial access across geographic regions, enables participation of Micro, Small, and Medium Enterprises (MSMEs) in the digital market, and offers more equitable services to underserved populations

You Are Here: It's More Than Being "Online"

You might think the digital divide only affects people without internet access. But this chapter shows that many people are "connected" yet still excluded, because data is expensive, skills are limited, platforms feel unsafe, or services are not designed for them. Being online does not always mean being included.

7.1 Understanding the Digital Divide in Southeast Asia

The evolution of technology offers opportunities, but it also exacerbates existing inequalities. One challenge in this context is the digital divide, the gap between individuals, communities, or nations in accessing, using, or benefiting from digital technologies. In Southeast Asia, this divide has implications for human rights, as it can threaten freedoms, deepen social inequalities, and hinder socio-economic growth.

Digital divide refers to a disparity in the economic capacity to access digital devices and services. This gap is not merely about physical access to technology but is also influenced by various socio-economic, geographic, and demographic factors, including gender, age, income, location, education, and communication infrastructure. The scope of the digital divide extends beyond individual access, affecting communities and nations by creating disparities in socio-economic growth.

7.1.1 Global and ASEAN Statistics

The digital divide remains a global issue, affecting billions of people despite recent progress. According to the International Telecommunication Union (ITU) 2025, the United Nations specialised agency for digital technology, around 2.2 billion people, most from low and middle-income countries, are still offline, revealing a disparity in digital access. Geographic disparities are clear. Signe in 2023 revealed that internet penetration is highest in Europe at 89%, followed by the Americas at over 80%, and the Arab States at 70%. However, Asia lags behind at 61%, while Africa is the lowest, at just 40%.

In Southeast Asia, about 77% of the region's population, approximately 460 million out of 600 million people, were online in 2022, a significant increase from 360 million in 2019 and 400 million at the onset of COVID-19 in 2020. This rapid growth reflects the surge in internet use during the pandemic, as people turned to online platforms for work, education, and commerce. Despite these developments, internet access remains uneven, leaving substantial segments disconnected, particularly in less developed areas. According to Sefrina, in 2024, Singapore, Thailand, and Malaysia stand out with over 80% of their populations online, showcasing their advanced digital infrastructure. In contrast, Laos, Myanmar, and Timor-Leste fall significantly behind, with only around a third of their populations connected.

The digital divide is further compounded by demographic disparities, with access differing significantly by gender, age, and location. Globally, about 69% of men used the internet in 2022, compared to 63% of women, leaving roughly 259 million more men than women online. Additionally, women are 7% less likely to own a mobile phone and 16% less likely to use mobile internet, creating a divide that results in 264 million fewer women. Youth connectivity rates are relatively high, with 75% of individuals aged 15-24 online, but a stark urban-rural gap persists, as internet users in urban areas are double those in rural areas.

In ASEAN countries, Woetzel et al., study viewed that gender equality in digital access has shown improvement compared to other parts of Asia. For example, Brunei reports near parity in mobile phone ownership and internet use, with women even surpassing men in both, as reported by Sey. However, digital gender gaps persist, particularly when intersecting with socioeconomic and geographic divides. In Indonesia and Thailand, digital infrastructure is heavily concentrated in urban centres, leaving rural communities underserved. Gender disparities in mobile phone ownership are more regionally visible in lower-income and rural areas, where women often rely on male family members for digital access. According to Sey's study, financial inclusion through mobile platforms also varies widely; while higher in Singapore, Malaysia, and Thailand, fewer than 35% of people in lower-income ASEAN countries access financial services through digital technology.

The digital divide marginalises diverse groups in ASEAN beyond women and rural populations. Jun E's study identified informal workers, micro, small, and medium enterprises (MSMEs), elderly people, people with disabilities, indigenous populations, and migrants as particularly vulnerable to this concern. Sefrina's study proposed that digital inequality in ASEAN spans multiple, often intersecting areas, creating layered barriers for different groups. These disparities include gaps in internet access and usage, income inequality within the digital economy, and limitations in digital skills and literacy. More importantly, they are often compounded by cultural and language differences, limited participation in STEM fields, restricted access to financial services, and concerns over online safety and security. Since these factors do not exist in isolation but intersect, they reinforce exclusionary cycles across the region.

Table 7.1 highlights the significant variation in internet access, digital literacy, and digital skills across Southeast Asia. According to World Bank data from 2023, on average, 75.64% of the population across the listed countries had internet access, but disparities remain. Brunei Darussalam (99%), Malaysia (98%), Singapore (94%), and Thailand (90%) have the highest internet penetration, while Timor-Leste lags far behind at 34%. Digital skills and talents rankings further illustrate regional gaps; Singapore ranks impressively at 12th globally, followed by Malaysia (33rd) and Thailand (45th), whereas Indonesia (51st) and the Philippines (54th) trail behind. These results suggest that while internet access is relatively high in several ASEAN countries, significant disparities in digital literacy and skills persist, potentially limiting the full economic and social benefits of digital connectivity, especially in lower-performing countries.

Table 7.1: Southeast Asia's Internet Access, Digital Literacy, and Digital Skills

Countries	Internet Access (% of Population)	Digital Skills & Talents Ranking (Out of 63 Global Countries)
Brunei Darussalam	99	N/A
Cambodia	61	N/A
Indonesia	69	51
Lao PDR	64	N/A
Malaysia	98	33
Myanmar	59	N/A
Singapore	94	12
Thailand	90	45
Timor-Leste	34	N/A
The Philippines	84	54
Vietnam	78	N/A
Average	**75.64**	**-**

7.1.2 Dimensions of the Digital Divide

To better capture the complexity of the digital divide, Buschmass et. al., working paper propose a six-dimensional framework comprising affordability, availability, digital education, digital security, environment, and resilience. (See Table 7.2)

Table 7.2: Dimensions of Digital Divide

Dimension	Description	Suggestive Variables
Affordability	Economic ability to access digital devices, data plans, and digital services.	Broadband operators' market share (fixed and wireless); Fixed-line monthly broadband cost/tariff; Mobile phone contract cost (post-paid/pre-paid tariff); Gross national income per capita (purchasing power parity)
Availability	Presence and reach of infrastructure such as electricity, mobile, and broadband networks.	Bandwidth capacity; Internet access; Access to computers; Network coverage (min. 2G, 3G, 4G, 5G); Mobile quality (upload/download speed, latency); Fixed-broadband quality (upload/download speed, latency)
Digital Education	Access to digital literacy, ICT tools, and skills development opportunities.	Level of literacy; Support for digital literacy; Mean years of schooling; Percentage of schools with Internet access; Secondary education gross enrolment rate; Tertiary education gross enrollment rate
Digital Security	Trust in digital platforms, data privacy, and protection from online threats.	e-Commerce safety; Trust in government websites and apps; Trust in information from social media; Trust in non-government websites and apps; Trust in online privacy; Secure Internet servers per million people
Environment	Wider socio-political and economic context shaping digital inclusion.	Democracy Index; Global Peace Index; EIU Business Environment Rankings; Global Gender Gap Index
Resilience	Ability of digital systems to remain functional during crises or disasters.	Inform Global Risk Index; Percentage of population covered by a recent hazard mitigation plan; Percentage of housing units covered by national flood insurance programme policies; National budget for disaster management (as ratio of informed risk score)

Affordability refers to the economic capacity to access digital devices and services, often constrained by high costs relative to income. Availability captures infrastructure-related gaps, including the presence of broadband networks, electricity, and mobile coverage. Digital education focuses on disparities in skills, literacy, and access to ICT-enabled learning environments. Meanwhile, digital security addresses privacy, trust, and protection against online threats, which influence individuals' willingness and ability to participate online. The remaining two dimensions emphasise systemic and contextual factors. The environment reflects the broader socio-economic and political conditions, such as gender bias, poverty, and political stability, that shape digital development. Resilience refers to the capacity of digital systems to withstand and function during crises, including natural disasters or political upheavals.

These six dimensions and their variables also help explain why digital inequalities persist across Southeast Asia. For instance, affordability relates to financial barriers such as the high cost of broadband plans or mobile phone contracts relative to income, which continue to limit access for many low-income households. Availability highlights the lack of, or unreliability of, infrastructure in remote areas, as evidenced by weak mobile network coverage, limited bandwidth capacity, or poor fixed-broadband speeds. Gaps in digital education are reflected in disparities such as the percentage of schools with internet access, mean years of schooling, or the lack of structured support for digital literacy. Digital security concerns, ranging from low trust in government websites and apps to limited secure internet infrastructure, can discourage individuals from engaging with digital services. Meanwhile, broader environmental factors, such as governance quality and gender equity, and resilience indicators, such as disaster preparedness budgets and digital inclusion in emergency protocols, shape how digital technologies reach and serve vulnerable populations. Therefore, the six dimensions not only describe the contours of digital exclusion but also point to its underlying causes and what must change to bridge the divide.

Reflection and Discussion

- *What does affordability mean in daily life when it comes to owning a smartphone or paying for internet data?*
- *Why might a student living in a rural village experience digital inequality even if they own a mobile phone?*
- *How does digital education affect a person's ability to use online banking, e-government services, or learning platforms?*
- *What kinds of online safety concerns might stop people from using apps, websites, or digital payments?*

7.1.3 What the Digital Divide across Southeast Asia Looks Like

Across ASEAN, the six dimensions of the digital divide are shaped by national income levels, geographic conditions, political structures, and digital governance models. According to the OECD 2023 report, Myanmar, Laos, and Cambodia continue to face significant challenges in availability and affordability, particularly in rural areas where mobile broadband coverage is limited and fixed-line internet remains prohibitively expensive relative to income. In both the Philippines and Indonesia, fragmented telecommunications infrastructure, geographic challenges, and uneven network coverage contribute to persistent issues with internet speed, reliability, and resilience, particularly in remote areas and during natural disasters. Singapore and Brunei generally score well on affordability and infrastructure-related indicators. However, digital security remains a concern, with both facing increased vulnerability to cyber threats and rising scepticism around data privacy. Although Vietnam has a high internet usage rate and ranks second only to Singapore in fixed broadband penetration and third in urbanisation levels, it still faces pronounced digital divides between urban and rural areas and between men and women. In Vietnam, restrictions on online speech and pervasive surveillance also contribute to low trust in government-controlled digital channels, weakening both digital participation and security.

Similarly, Malaysia and Thailand may share stronger broadband penetration, particularly in mobile broadband, than some ASEAN members, yet inequalities persist. In Malaysia, half of the population experiences poor internet connectivity, partly because over half of the country's telecommunications towers are concentrated in just four states, hindering efforts to achieve nationwide 5G goals. Although Thailand has an extensive terrestrial fibre network connecting major urban centres, only 19% of the population lives within 10 km of a transmission node, posing significant barriers to extending broadband coverage to sparsely populated areas. These trends highlight the need for targeted, rights-based digital policies that respond to country-specific vulnerabilities across all six dimensions.

While the six dimensions of affordability, availability, digital education, digital security, environment, and resilience provide a framework for mapping the manifestations of the digital divide in Southeast Asia, they are deeply intertwined with broader systemic issues that perpetuate exclusion. These dimensions do not operate in isolation; instead, they are exacerbated by underlying structural gaps in economic-technological, political-legal, and social-cultural spheres, which hinder equitable access to digital rights and opportunities. Addressing these interconnected barriers is essential for advancing human rights in the region, as explored in the following section.

Case Study: Digital Divide between Urban and Rural Citizens in Thailand

A study in Thailand revealed that approximately 83.8% of the population had internet access in 2021. Improved digital access has brought benefits to urban and some rural communities, with telemedicine services like Doctor Raksa and Mor Prom expanding healthcare access, and digital payments and online platforms aiding small businesses.

However, significant gaps persist, particularly between urban areas like Bangkok, which boasted 93.8% connectivity, and other regions. This divide hindered many from fully benefiting from government programs; for instance, the "Rao Chana" (We Win) initiative provided financial aid during the COVID-19 pandemic but required online registration, leaving many in rural and mountainous areas unable to access the program. These individuals had to seek alternatives, such as in-person registration, incurring additional costs and time burdens. The demographic most likely to engage with e-government services included females aged 25-42, residing in cities, holding an undergraduate degree, and using 5G broadband technology. This case demonstrates how digital disparities, even with high overall internet penetration, can create inequalities in access to essential services and opportunities.

Reflection and Discussion:

Thailand's urban centers like Bangkok, enjoy near-universal internet access, while rural provinces still face limited infrastructure, affordability barriers, and skills gaps. This creates unequal opportunities for education, economic participation, and civic engagement.

- *What are the human rights implications of this digital divide?*
- *How will it impact someone's education?*
- *Will it change work and employment?*
- *What strategies, technological, legal, and social, could help bridge this gap while respecting human rights principles?*

7.2 Structural Gaps Reinforcing Digital Inequality

Beyond the six dimensions discussed earlier, the digital divide in Southeast Asia stems from three broader structural gaps: economic-technological, political-legal, and social-cultural. These gaps overlap and cut across all dimensions, worsening inequalities in access, participation, and governance. Simply put, the divide is not just about technology; it is about how these interconnected issues reinforce broader social, economic, and political barriers. Let's break down the three key gaps:

- *Economic-Technological Gaps:* These refer to disparities in access to advanced information and communication technologies (ICTs) that can exclude regions from technological and economic progress.
- *Political-Legal Gaps:* These are disparities deepened by political and legal frameworks in digital governance, including issues like digital authoritarianism, censorship, and weak legal protections that suppress online freedoms and limit equitable access to information.
- *Social-Cultural Gaps:* These refer to consequences that reinforce and exacerbate existing inequalities, such as poverty, gender inequality, and marginalisation, by limiting access to digital education, healthcare information, and social protection services.

7.2.1 Economic-Technological Gaps

Economic-technological gaps in Southeast Asia refer to disparities in access to advanced information and communication technologies (ICTs) that exclude people, places, and groups from technological and economic progress. Internet penetration in Southeast Asia is increasing, largely driven by smartphone adoption and improvements in internet infrastructure. Despite this progress, significant disparities in digital infrastructure persist, particularly between urban and rural areas, hindering broader participation in the digital economy. The disparities between high-penetration countries like Singapore from low penetration like Laos are influenced by factors such as internet speed, internet usage, and technology production, with high-income ASEAN Member States (AMS) enjoying top-tier internet speeds and near-universal access, while lower-income countries experience severe limitations.

This gap impacts Micro, Small, and Medium Enterprises (MSMEs), which form the backbone of ASEAN economies. MSMEs frequently encounter barriers such as limited business knowledge, inadequate ICT skills, high implementation risks and costs, and a lack of localised support, all of which hinder their digital adoption efforts. As global and regional markets move online, the divide between digitally enabled and digitally excluded MSMEs widens. The result is income inequality and slowing inclusive growth. Moreover, employees in digitally disadvantaged areas have reduced access to training and professional development, missing crucial opportunities to reskill and upskill in digital economy competencies like data literacy and cybersecurity.

Technological advancements also lead to market concentration by some companies, such as tech giants, giving larger firms a competitive edge and making it difficult for MSMEs and startups to compete. The result is that consumers' interests may not be met, they may face less data protection, and the workers in this area may have less rights. The rise of AI technologies further complicates this by giving an advantage to the dominant companies. In Southeast Asia, dominant e-commerce platforms such as Lazada, Shopee, and Grab rely on vast amounts of personal data which can be leveraged by AI-driven data analytics to outcompete smaller businesses who struggle to adopt similar tools due to high costs.

7.2.2 Political-Legal Gaps

Political-legal gaps deepen the digital divide in Southeast Asia, driven by disparities in digital governance. Digital authoritarianism is increasingly prevalent in the region, with governments restricting and removing online content under the guise of combating fake news and disinformation. Countries in Southeast Asia often blend authoritarianism, characterised by extensive surveillance and regulation aimed at maintaining social harmony. A country might have high levels of surveillance and control over digital information. The country's control over digital infrastructure, through measures such as internet filtering, shutdowns, and social media monitoring, may limit equitable access to information and suppress online freedoms. For instance, Thailand's Computer Crime Act criminalises criticism of the monarchy, the military, and certain political groups. Vietnam enforces content removal under its Cybersecurity Law, and Myanmar's military has imposed repeated internet shutdowns to suppress dissent. The principle of non-interference prevalent in the region also limits collaborative efforts to foster large-scale, inclusive participation in digital governance.

Many Southeast Asian countries have significantly strengthened their control over digital infrastructure. Income levels do not solely determine this capability; for example, Myanmar, one of the region's poorest nations, possesses comparable, and sometimes superior, social media monitoring capabilities to wealthier countries like Singapore, indicating that repression is often driven by political control needs rather than economics. The COVID-19 pandemic further exemplified this trend, with many ASEAN countries using surveillance, censorship, and misinformation under emergency laws to stifle dissent. High-profile cases, such as Maria Ressa's cyber libel conviction in the Philippines and Malaysia's fining of Malaysiakini, illustrate how regimes employ cyber laws to silence critics, reinforcing an "illiberal alliance" within ASEAN.

Digital infrastructure manipulation and information operations (IOs) enhance state control over online spaces, deepening digital repression. In Thailand, authorities have reportedly coordinated information operations by deploying fake social media accounts to amplify pro-government narratives and discredit activists. Authoritarian regimes often exacerbate issues such as limited competition within the broadband value chain, prioritising corporate interests and promoting surveillance capitalism, in which companies collect vast amounts of user data, analysed by AI, to predict and shape human behaviour. In Indonesia, the rapid growth of e-commerce platforms has led to widespread collection of personal data with limited consumer protections.

Politically motivated control often reinforces weak legal protections, despite 88% of ASEAN nationals being covered by comprehensive data protection laws. The uneven implementation and weak enforcement of these laws create disparities in the ability to access and participate in digital spaces safely. While the ASEAN Framework on Personal Data Protection, adopted in 2016, aimed to establish common principles, significant challenges persist in ensuring individuals can trust and control their personal data. The surge in data breaches and cyberattacks in countries further highlights weaknesses in digital security infrastructure, disproportionately affecting users who already face barriers to digital access. These limitations lead to a deepening digital divide, as marginalised communities struggle to access reliable information or participate online, reinforcing existing social and economic inequalities. Table 7.3 is adapted from the Freedom House report on internet freedom. The average score is 41.9 out of 100, indicating serious restrictions on online freedom across the region. Countries such as Myanmar and Vietnam score particularly low, especially in areas related to content restrictions and violations of user rights. Data for Laos, Timor-Leste, and Brunei is not available in the report. Internet freedom scores are measured out of 100 and are based on three main areas: access to the internet, limits on online content, and violations of user rights.

Table 7.3: Southeast Asia's Internet Freedom Scores

Countries	Overall	Limits on Content	Violations of User Rights
Cambodia	43	16	14
Indonesia	49	18	16
Malaysia	60	21	20
Myanmar	9	5	2
Singapore	53	17	17
Thailand	39	14	9
The Philippines	60	23	21
Vietnam	22	6	4
Average	**41.9**	**15**	**12.9**

Case Study: Legal-Political Barriers to Digital Participation in the Philippines

Maria Ressa, CEO of the news site Rappler, and writer Reynaldo Santos Jr. were convicted under Section 4(c)(4) of the Philippines' 2012 Cybercrime Prevention Act (CPA). The charges stemmed from a 2012 article that alleged a businessman's involvement in human trafficking and drug smuggling. Although the article was published months before the CPA's enactment, the court ruled it was "republished" in 2014 due to a minor correction, making it subject to the CPA's cyber libel provisions. Ressa and Santos received prison sentences of up to six years and a fine of 200,000 PHP (approximately 4,000 USD).

This conviction was widely seen as part of a pattern of harassment against critical media by the Duterte administration, particularly those reporting on the government's violent "war on drugs". The ruling established new legal precedents for libel, including a 12-year period to complain, compared to the one-year limit for traditional libel, and raised concerns over prosecutions of articles before the law was in place. Human rights advocates argued that this precedent contradicts principles in Article 15 of the International Covenant on Civil and Political Rights (ICCPR), which prohibits retroactive criminal liability.

Reflection and Discussion:

1. *The conviction of Maria Ressa under the Cybercrime Prevention Act was criticised for violating legality because it was an act of retroactive criminal liability. What does this mean, and why is it wrong to apply a law retroactively? How do such legal applications impact the rule of law in the digital sphere, especially in Southeast Asia?*
2. *This case is limiting press freedom and freedom of expression. What are the consequences when governments use cyber laws to silence journalists and activists for online content?*

Case Study: Malaysia's Fining of Malaysiakini

Malaysiakini, an online news platform, published a report where subscribers posted comments criticising the judiciary's independence and the Chief Justice. The Malaysian Federal Court found Malaysiakini guilty of criminal contempt due to the five user comments. Despite promptly removing the comments upon police notification, Malaysiakini was fined RM500,000 (approximately 122,700 USD), a sum far exceeding the prosecution's recommendation. The court cited Malaysiakini's presumed liability under Section 114A of the Evidence Act, which holds intermediaries accountable for third-party content unless rebutted.

Critics argued that this standard is incompatible with international human rights norms and violates principles of legality, necessity, and proportionality, particularly given the lack of clear definitions for contempt of court in Malaysian law. This case highlighted challenges to online freedom of expression and press freedom. The ruling means smaller media outlets are far more vulnerable than wealthier organizations who can pay these costs. Smaller platforms and marginalised voices risk exclusion from online expression and justice systems.

Reflection and Discussion:

Malaysia's Federal Court fined Malaysiakini for user comments, citing liability under Section 114A of the Evidence Act. Should the media be liable for its readers' comments? How can a balance be struck between accountability for harmful content and protecting legitimate online discourse?

This case highlighted how rulings like this create a digital divide between small and large media companies. Why is this bad? What is the importance of having small media platforms? What can they do which large media corporations cannot?

7.2.3 Social-Cultural Gaps

The digital divide also carries social consequences, reinforcing existing inequalities such as poverty, gender inequality, and marginalisation. Groups with low levels of internet penetration also tend to have lower Human Development Index (HDI) scores, particularly in Least Developed Countries (LDCs). Limited digital access restricts individuals' ability to benefit from increasingly digitised education, healthcare information, and social protection services.

The UNICEF *Global Disability Inclusion Report 2025* highlights that digital inclusion remains limited among marginalised groups, including women, rural populations, older adults, and individuals with lower income or education levels. Gender gaps in ASEAN are wider in advanced areas of digital economy participation, such as skills, entrepreneurship, and STEM careers, than in basic digital access. Research indicates that women face greater barriers to acquiring digital skills and accessing ICT opportunities than men do. In Indonesia, for example, low digital literacy among urban and rural women increases their vulnerability to online risks, such as predatory loan schemes. Beyond gender, other factors contributing to digital exclusion in Southeast Asia include disability, illiteracy, age, income level, urban economic concentration, and limited enterprise access to capital. UNICEF also reported that persons with disabilities, for instance, face heightened barriers due to lower disposable income, limiting their ability to afford digital devices and essential services like internet access, electricity, and equipment maintenance.

The integration of artificial intelligence (AI) into digital ecosystems further amplifies social-cultural gaps in Southeast Asia, where biased algorithms often reinforce existing inequalities such as poverty, gender disparities, and ethnic marginalisation. For instance, large language models (LLMs) and AI systems are predominantly trained on Eurocentric or Western datasets rather than on Southeast Asian training data. This may lead to flawed outcomes like inaccurate speech and image recognition for local languages, dialects, or indigenous features, disproportionately affecting rural women, ethnic minorities, and indigenous populations. This bias not only widens the digital divide by excluding underrepresented groups from effective use of AI-driven services but also perpetuates cultural erasure and discrimination in areas like education and healthcare. From a human rights perspective, these issues underscore the need for protections such as the "right to explanation," which allows individuals to demand transparency into how AI decisions are made to challenge biases and ensure non-discrimination.

7.3 A Human Rights-Based Approach (HRBA) to Digital Inclusion

One method to address these disparities is to apply a Human Rights-Based Approach (HRBA). This approach integrates human rights principles, such as equality, participation, non-discrimination, and accountability, into a framework to better understand, and work towards bridging the digital gap and create inclusivity.

7.3.1 Four Spheres of Digital Rights

To better understand the digital divide, Table 7.4 shows four distinct spheres of digital rights adapted from Jun E. work, which includes: Digital Space, Data Representation, Access, and Governance. These spheres operate under both "digital" and "developmental" paradigms.

- *Digital Space* encompasses fundamental freedoms and protections online, mirroring rights enjoyed offline. This includes the freedom of expression, association, and assembly online, as well as the right to exist free from violence, hateful speech, and harassment. The UN Human Rights Council Resolution 68/167 (2013) affirms this principle, stating that "The same rights that people have offline must also be protected online".
- *Data Representation* focuses on rights related to personal data in the digital realm. Key aspects include the right to data privacy, the right to freedom from digital surveillance, and the right to non-discrimination in the collection and use of data. This sphere also covers informed consent for participation, data ownership and control, and the right to data security and protection. Weak protections in this area leave marginalised groups particularly vulnerable.
- *Access* emphasises the necessity of equitable access to technology and digital services to benefit from scientific progress. This includes the right to access state and other services online, the right to access the Internet, and the right to access hardware/software. Meaningful access extends beyond connectivity to include affordability, digital literacy, and locally relevant content.
- *Governance* pertains to the inclusive participation of individuals in decisions which shape digital spaces and internet policy. This sphere highlights the right to participate in digital governance processes and to be consulted on internet policy issues.

Table 7.4: Four Spheres of Digital Rights

Digital Rights		Digital Development Rights	
Digital Space	**Data Representation**	**Access**	**Governance**
• Freedom of expression, association, and assembly online • Right to consumer protection • Right to seek joy and pleasure • Right to exist free from violence, hateful speech, and harassment • Right to non-discrimination • Right to have informed consent on participation	• Right to data privacy • Right to freedom from digital surveillance • Right to data ownership and control • Right to data security and protection	• Right to access state and other services online • Right to access the Internet • Right to access information and content • Right to access hardware/software	• Right to participate in digital governance processes or be consulted on Internet policy issues

7.3.2 Alignment with Core HRBA Principles

The convergence of the HRBA with these four spheres of digital rights offers a framework for addressing the digital divide by centring human dignity, justice, and inclusion in digital policy and practice. Each sphere aligns with the core HRBA principles of equality, participation, non-discrimination, and accountability (See Table 7.5).

- *Equality* in the context of digital rights means ensuring equal participation in online environments for all individuals, promoting fair and inclusive data systems, and bridging digital gaps based on income, gender, and geography. It also guides equitable policy design and implementation in digital governance.
- *Participation* ensures that individuals have a voice in the digital sphere. This is reflected in the freedom of expression and online engagement, the inclusion in data governance processes, and community involvement in digital inclusion programs. At an institutional level, it should include participatory decision-making to ensure diverse perspectives are considered.

- *Non-Discrimination* is vital for safeguarding vulnerable populations in the digital age. This principle entails protection against online exclusion, harassment, and hate speech, the prevention of algorithmic bias and discriminatory profiling, and ensuring inclusive access regardless of identity or status. It also emphasises legal guarantees for vulnerable and underrepresented populations.
- *Accountability* ensures that duty-bearers are responsible for their actions and omissions in the digital realm. This includes establishing accessible redress mechanisms for online rights violations, ensuring transparent data collection and usage, monitoring service provision, ensuring affordability, and maintaining justice when enforcing digital rights and standards.

Through this alignment, HRBA provides a foundation for transforming digital inequality into digital justice. This is not just the technical aspects of the digital divide but also the way people use digital technology.

Table 7.5: Mapping HRBA Principles onto the Four Spheres of Digital Rights

HRBA Principle	Digital Space	Data Representation	Access	Governance
Equality	Equal participation in online environments	Fair and inclusive data systems	Bridging digital gaps based on income, gender, and geography	Equitable policy design and implementation
Participation	Freedom of expression and online engagement	Inclusion in data governance processes	Community involvement in digital inclusion programs	Multi-stakeholder decision-making at institutional levels
Non-Discrimination	Protection from exclusion, harassment, and hate speech online	Prevention of algorithmic bias and discriminatory profiling	Inclusive access regardless of identity or status	Legal guarantees for vulnerable and underrepresented populations
Accountability	Accessible redress mechanisms for online rights violations	Transparent and regulated data collection and usage	Monitoring and reporting on service provision and affordability	Oversight institutions to enforce digital rights and standards

Case Study: Empowering Environmental Justice through Digital Technology

The FireD (Fire Detection Application) project in Chiang Mai, Thailand, serves as a successful example of a Human Rights-Based Approach to digital access.

Chiang Mai, in Northern Thailand, annually suffers from severe air pollution, particularly during the dry season, due to a range of causes, including agricultural burning, forest fires, and pollution from traffic and factories. This poses serious health threats, especially for rural communities that often have limited access to healthcare and real-time information on air quality. Historically, efforts to combat open burning were top-down and reactive, lacking meaningful citizen participation, where the government told people what to do, but never listened to them. Addressing this gap required digital tools that were accessible, community-driven and supportive of public health and environmental protection.

The FireD project responded to this need by launching a mobile-based platform that enables citizens to report incidents of open burning and forest fires directly to local authorities. The application was designed to be free to use and compatible with low-cost smartphones, ensuring its accessibility for users in remote areas. It integrates satellite data, real-time fire detection, and community reporting functions. Citizens become active environmental monitors. Through digital literacy training workshops, community members, including farmers, youth, and elderly residents, were equipped to use the app.

This initiative demonstrates "meaningful access" by combining digital literacy, affordable technology, and relevant content to protect public health. The FireD application strengthens the right to a healthy environment and promotes citizen participation in public affairs, which are core elements of climate justice and the broader HRBA. By providing community members, including marginalised rural populations, with access to information and a platform for action, it narrows the rural-urban information gap and ensures non-discrimination. The success of FireD illustrates how targeted, rights-based digital interventions can bridge not only the digital divide and social and political inequalities.

Reflection and Discussion:

The FireD project demonstrates a Human Rights-Based Approach (HRBA) to digital inclusion. What were the most significant features of the FireD application which addressed the dimensions of:

- *Affordability,*
- *Availability,*
- *Digital education,*
- *Right to a clean environment.*

7.4 Alternative Approaches to Bridge the Digital Divide

Beyond government programmes, alternative governance mechanisms have been introduced to help bridge the digital divide in everyday life. These include partnerships between governments, businesses, civil society organisations, and local communities, as well as initiatives that expand access to digital financial services. Such approaches aim to improve accountability, address gaps in regulation and service delivery, and support marginalised communities in participating more fully in digital economic activities and decision-making processes.

7.4.1 Multi-stakeholder Collaboration

Digital governance relies on collaboration among the public sector, private sector, and civil society organisations. This multi-stakeholder approach ensures that digital spaces remain open, rights-respecting, and accessible to all.

- The public sector, primarily governments, is responsible for policy-making, legislation, and the development of digital infrastructure. Their role involves creating the overarching regulatory environment and foundational infrastructure that support digital development.
- The private sector contributes through innovation, investment, and compliance with regulatory frameworks. Technology companies drive technological advancements and provide digital services, making them partners in expanding digital access and opportunities.
- Civil society organisations (CSOs) play a role in holding both the public and private sectors accountable, conducting independent research, educating the public, and facilitating community engagement. They serve as watchdogs and advocates, ensuring that technology promotes positive change while mitigating harm, especially for marginalised groups.

By working together, these stakeholders can design and implement regulatory frameworks that are inclusive and responsive to diverse perspectives.

7.4.2 Digital Finance Inclusion

The digital finance sector in ASEAN has experienced rapid growth, with services such as digital banking, mobile payments, and online lending becoming increasingly widespread. Countries like Singapore, Indonesia, and Malaysia have emerged as regional FinTech hubs, attracting substantial local and international investment. The popularity of e-wallets such as GoPay, GrabPay, and OVO, along with the rise of QR code payments, is accelerating cashless transactions and financial inclusion across the region.

However, while this growth may develop “Inclusive Digital Economy” by expanding financial access across geographic regions, there are still challenges of accessibility for MSME participation in the digital market, as well as other marginalised groups.. While rising income levels can address affordability, achieving an inclusive digital economy also requires tackling income inequality and ensuring quality broadband connectivity. This can be impeded by varying internet speeds and regulatory issues, particularly those related to consumer protection and data governance.

Case Study: The Digital Finance Inclusion Initiative in Indonesia

In Indonesia, a successful model of digital financial inclusion has emerged through collaboration between the government, the private sector, and civil society organisations. The National Strategy for Financial Inclusion (SNKI), launched in 2016, actively promotes partnerships between government agencies, FinTech companies, and community organisations to improve access to digital banking and financial services, particularly in rural and underserved areas.

Supported by the Asian Development Bank (ADB) and Germany’s KfW through the Promoting Innovative Financial Inclusion Program, this initiative has grown the digital payments ecosystem. Platforms like GoPay, OVO, DANA, and LinkAja play a central role by offering accessible, app-based services integrated with e-commerce, transportation, and retail networks. This public-private partnership (PPP) model demonstrates how alternative mechanisms can effectively bridge digital gaps, promote inclusive economic participation, and build trust in digital systems, aligning with a Human Rights-Based Approach (HRBA) to digital governance.

Reflection and Discussion:

What Human Rights-Based Approach principles (equality, participation, non-discrimination) should be considered when addressing access to online financial tools for marginalised populations such as persons with a disability, people who may not speak or read the national language, or the elderly?

You Are Here: The Future Is Not Automatic

A more inclusive digital Southeast Asia will not happen automatically through technology alone. It depends on choices, about law, design, education, and accountability. Understanding the digital divide gives you the tools to question these choices and push for fairer outcomes

7.5 Conclusion

This chapter examines the digital divide in Southeast Asia, defining it as a disparity in access to, use of, and benefit from digital technologies, influenced by socio-economic, geographic, and demographic factors. ASEAN statistics reveal an uneven internet penetration and disparities across countries and vulnerable groups. The divide can be categorized into six dimensions: affordability, availability, digital education, digital security, environment, resilience. There are three structural gaps in reinforcing digital inequality: economic-technological , political-legal, and social-cultural. The chapter overviews on way to approach these concerns through a Human Rights-Based Approach to digital inclusion, aligning digital rights (Digital Space, Data Representation, Access, Governance) with core HRBA principles, and exploring alternative approaches like multi-stakeholder collaboration and digital finance inclusion.

Key Takeaways

1. The digital divide in Southeast Asia refers to the gap in accessing, using, or benefiting from digital technologies, driven by socio-economic, geographic, and demographic factors, with implications for human rights and socio-economic growth.
2. While internet penetration in ASEAN increased, access remains uneven, with countries like Singapore showing high connectivity while Laos, Myanmar, and Timor-Leste significantly lag, and digital gender gaps persist especially in rural and lower-income areas.
3. The digital divide is reinforced by three structural gaps: economic-technological (disparities in ICT access), political-legal (digital authoritarianism), and social-cultural (poverty, gender inequality, and marginalization limiting access to digitized services).
4. A Human Rights-Based Approach (HRBA) to digital inclusion aligns principles of equality, participation, non-discrimination, and accountability across four spheres: Digital Space, Data Representation, Access, and Governance.
5. Alternative approaches to bridging the divide include multi-stakeholder collaboration (public, private, civil society), digital finance inclusion (FinTech, e-wallets).

Issues to Think About

1. How has the digital divide personally affected your access to education or jobs in Southeast Asia, and what one change could make it fairer for you?
2. In your country, how do political-legal gaps like censorship impact young voices online, and what rights-based steps could protect them?
3. Imagine applying HRBA to include people with disabilities in digital spaces. How might that transform communities in your region?
4. What role could you play in a multi-stakeholder effort to boost digital finance for rural MSMEs, drawing from examples like Indonesia's initiatives?
5. If social-cultural gaps widen poverty through tech exclusion, how can we ensure apps and services respect diverse languages and cultures in ASEAN?

Further Readings

ASEAN Foundation. (2024). *One divide or many divides: Underprivileged ASEAN communities' meaningful digital literacy and response to disinformation*. https://aseanfoundation.org/wp-content/uploads/2024/03/ASEAN_DLP_Research_Report_-_One_Divide_or_Many_Divides.pdf

ASEAN. (2025). *ASEAN digital community 2045: Country perspectives*. Economic Research Institute for ASEAN and East Asia. https://www.eria.org/uploads/ADC-2025-Country-Perspectives.pdf

ASEAN. (2025). *ASEAN digital masterplan 2025*. https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf

Buschmaas, J., Chan, C., Mendler, L., Qi, C., & Senkpiel, H. (2019). *Measuring the digital divide in the Asia-Pacific region for the United Nations Economic and Social Commission for Asia and the Pacific* (AP-IS Working Paper Series). United Nations Economic and Social Commission for Asia and the Pacific. https://www.unescap.org/sites/default/files/Measuring%20the%20Digital%20Divide%20in%20the%20Asia-Pacific%20Region%20for%20the%20United%20Nations%20Economic%20and%20Social%20Commission%20for%20Asia%20and%20the%20Pacific_0.pdf

EU-ASEAN Business Council. (2020). *Data governance in ASEAN: From rhetoric to reality*. https://www.eu-asean.eu/wp-content/uploads/2022/02/DATA-GOVERNANCE-IN-ASEAN-FROM-RHETORIC-TO-REALITY-2020.pdf

Freedom House. (n.d.). *Countrie and Territories – Internet freedom scores*. https://freedomhouse.org/countries/freedom-net/scores

International Telecommunication Union. (2025). *Measuring digital development: Facts and figures 2025*. https://www.itu.int/itu-d/reports/statistics/facts-figures-2025/

International Telecommunication Union. (2025). *State of digital development and trends in Asia and the Pacific: Challenges and opportunities*. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-SDDT_ASP-2025-PDF-E.pdf

Jun-E, T. (2019). Digital rights in Southeast Asia: Conceptual framework and movement building. In Y. H. Khoo & D. Simandjuntak (Eds.), *Exploring the nexus between technologies and human rights: Opportunities and challenges in Southeast Asia*. SHAPE-SEA. https://shapesea.com/wp-content/uploads/2025/07/SS-Technology-and-Human-Rights.pdf

McDermott, G. (2022). From the editor: The spectre of digital authoritarianism for Southeast Asia. *Kyoto Review of Southeast Asia*, Issue 33. https://kyotoreview.org/issue-33/from-the-editor-the-spectre-of-digital-authoritarianism-for-southeast-asia/

Organisation for Economic Co-operation and Development. (2023). *Extending broadband connectivity in Southeast Asia*. OECD Publishing. https://doi.org/10.1787/b8920f6d-en

RMIT University. (2025). *The future of ASEAN's digital economy depends on what we build today*. https://www.rmit.edu.vn/news/all-news/2025/nov/the-future-of-asean-digital-economy-depends-on-what-we-build-today

Sefrina, M. (2024). *An inclusive digital economy in the ASEAN region* (ERIA Discussion Paper Series No. 505). https://www.eria.org/uploads/An-Inclusive-Digital-Economy-in-the-ASEAN-Region.pdf

Sey, A. (2021). *Gender digital equality across ASEAN* (ERIA Discussion Paper Series No. 358). https://www.eria.org/uploads/media/discussion-papers/Gender-Digital-Equality-Across-ASEAN.pdf

Signé, L. (2023). *Fixing the global digital divide and digital access gap*. Brookings. https://www.brookings.edu/articles/fixing-the-global-digital-divide-and-digital-access-gap/

Springer. (2025). *State of digitalization in the Southeast Asia region – bibliometric review*. https://link.springer.com/article/10.1007/s11135-025-02296-3

Sriyai, S. H. (2024). *How means for digital repression in Southeast Asia have unfolded in recent times* (ISEAS – Yusof Ishak Institute Perspective No. 65). https://www.iseas.edu.sg/wp-content/uploads/2024/08/ISEAS_Perspective_2024_65.pdf

UNICEF. (2025). *Global Disability Inclusion Report 2025: Accelerating disability inclusion in a changing and diverse world*. https://www.globaldisabilitysummit.org/wp-content/uploads/2025/03/GIP03351-UNICEF-GDIR-Full-report_Proof-4.pdf

United Nations Development Programme. (2025). *UNDP warns: AI could trigger a new global divide without urgent action*. https://www.sustainabilitymenews.com/technology/undp-warns-ai-could-trigger-a-new-global-divide-without-urgent-action

United Nations. (2024). *International community must address digital gap between developed, developing states, speakers stress, as second committee takes up information technology*. https://press.un.org/en/2024/gaef3608.doc.htm

United Nations. (2024). *Secretary-General stresses Association of Southeast Asian Nations role as 'bridge builder' in peace, digital connectiveity*. https://press.un.org/en/2024/sgsm22407.doc.htm

World Economic Forum. (2022). *Bridging Southeast Asia's digital divide to drive financial inclusion*. https://www.weforum.org/stories/2022/05/bridging-southeast-asia-digital-divide-driving-financial-inclusion/

World Economic Forum. (2025). *Why ASEAN's new digital economy framework agreement is a gamechanger*. https://www.weforum.org/stories/2025/05/asean-digital-economy-framework-agreement-a-gamechanger/

Chapter 8:

Challenges of Governing Emerging Technologies and Protecting Human Rights

Reader's Guide

This chapter invites you to look beyond the excitement of emerging technologies and focus on the challenges of governing them responsibly. While tools such as artificial intelligence and automated systems promise efficiency and innovation, they also raise difficult questions about transparency, accountability, environmental impact, and human dependence, questions that existing laws often struggle to answer. As you read, you will explore why technological change frequently moves faster than regulation, how "black box" systems make decisions hard to explain or challenge, and how data-driven technologies can cause real harm when errors or biases go unchecked. The chapter also highlights less visible issues, including rising energy costs, uncertainty over responsibility, and governance gaps in Southeast Asia. In this chapter, you will:

- Understand why governing emerging technologies is especially challenging.
- Recognise how opacity, automation, and data dependence affect accountability.
- Identify the human, social, and environmental risks linked to new technologies.
- Reflect on why these governance challenges matter for human rights in Southeast Asia.

By the end of this chapter, you are encouraged to think critically about what it means to govern emerging technologies in a way that protects human rights.

Key Terms

- **Governance Gap**: The disparity between the pace of technological innovation and the often slow and deliberate legislative response, leading to new innovations being deployed without adequate safeguards.
- **Regulatory Arbitrage**: A situation where foreign companies exploit weaker regulations in certain countries to gain competitive advantages due to fragmented and inconsistent international regulatory frameworks.
- **Autonomous Weapons Systems (AWS)**: AI systems designed to select and engage targets without human intervention, raising fundamental questions about the morality of delegating life-and-death decisions to machines.
- **Cognitive Erosion**: The potential diminishment of critical human skills and overall human agency due to the reliance on AI technologies, such as navigation systems impairing spatial awareness.
- **Intellectual Property Rights (in Generative AI)**: Refers to the legal challenges surrounding authorship and ownership of works created by AI systems, as well as concerns about copyright infringement from data scraping copyrighted materials for AI training

The advent of emerging technologies, particularly Artificial Intelligence (AI), has brought opportunities for societal advancement, yet it also introduces challenges regarding their governance. The pace of innovation, coupled with the inherent complexities and global reach of these technologies, often strains traditional legal and rights-based frameworks. This chapter explores the challenges of regulating emerging technologies and the issues policymakers, legal experts, and society at large must address to ensure that technological progress aligns with human rights and societal well-being.

8.1 Challenges in Regulating Emerging Technologies

The regulation of emerging technologies, especially AI, presents new challenges stemming from their development, complexity, and the evolving landscape of legal and rights-based considerations.

8.1.1 Rapid Pace of Innovation vs. Slow Legislative Response

One challenge in governing emerging technologies is the governance gap, the disparity between the pace of technological innovation and the often slow and deliberate legislative response. Laws designed for stability may struggle to keep pace with the fast-evolving, highly technical issues posed by technologies such as artificial intelligence, big data, and blockchain. This means that innovations are often deployed without adequate safeguards, increasing the risk of misuse, harm, and human rights violations.

The democratic lawmaking process frequently lags behind technological progress. Contributing to this delay is the lack of technical expertise within public institutions, which limits their ability to effectively address critical digital rights issues such as data privacy, cybersecurity, and algorithmic bias. Consequently, regulations can quickly become outdated.

You Are Here: You're Using Technology Before Anyone Agreed on the Rules

The AI tools you use for studying, searching, writing, or entertainment often exist in a grey area where laws are unclear or still being debated. You are already adapting your behaviour to these technologies, even though society has not fully decided how they should be governed.

8.1.2 Complexity and Opacity of AI

The complexity of many AI systems is due to their opacity or what is known as the 'black box' phenomenon: no one knows what goes on inside as it is difficult, if not impossible, to look inside them to understand what is going on. AI does not operate like a program or equation which can be measured and modified. AI programs evolve and adapt as they operate, so what the program starts with is changed as it learns and evolves. AI is more like planting a forest: after seeds are sown, no one will know what the final forest will look like, nor what animals will live it. At least with a forest, people can see it grow. For an AI, nobody can see inside it.

This poses significant hurdles for effective regulation. Unlike traditional technologies that are more easily understood and controlled, advanced AI models, particularly those involved in deep learning, often operate as "black boxes". Their internal workings and decision-making processes are not easily interpretable or transparent to humans, making it challenging to understand how they arrive at their conclusions or recommendations.

Furthermore, the probabilistic nature of AI introduces uncertainty, as outcomes are based on statistical models rather than deterministic logic. This unpredictability complicates efforts to predict its behaviour and establish clear accountability in cases of errors or harmful outcomes. The vagueness and non-transparency of AI systems also complicate efforts to control it since it is difficult to assess whether an AI system conforms to existing laws or ethical standards. For example, early drafts of the European Union's proposed AI Act struggled to adequately address emerging technologies such as large language models and generative AI, highlighting a gap between legal standards and technological advancements. The lack of technical expertise among local lawmakers further hinders their ability to understand complex AI systems enough to comply.

8.1.3 Jurisdictional Limitations and Enforcement Issues

AI technologies are not limited by national borders. Single countries cannot enforce laws effectively. Because AI has a global reach, the law faces jurisdictional limitations (States cannot enforce their laws in other States) and enforcement issues (States rely on their own police forces, not those of other States). There is a risk of fragmented laws as nations develop diverse frameworks. For instance, the U.S. has a decentralised approach across different States, ministries, and self-regulation, whereas China has a state-controlled model. This patchwork approach can create confusion for legal practitioners and businesses operating in multiple regions.

The absence of a universally accepted definition of AI further creates complications. Cross-border issues, such as determining which country's privacy protections apply to international data flows, add another layer of complexity. Corporations can exploit these weaknesses in the law. This discrepancy can lead to a 'race to the bottom' or regulatory arbitrage, in which foreign companies exploit weaker laws in certain countries to gain a competitive advantage.

You are here: One Technology, Many Rules

The same AI system behaves differently depending on where it operates, not because the code changed, but because the rules did. For businesses, this means navigating legal uncertainty. For people, it means your rights may quietly expand or disappear when you cross a digital boundary you cannot see.

8.1.4 Accountability and Liability

The question of accountability and liability in AI systems is another challenge, especially as these systems gain the ability to make independent and autonomous decisions with potentially substantial consequences. When an AI system causes harm due to faulty programming or unintended consequences, conventional legal systems struggle to determine who should be held responsible. Recent cases include AI chatbots which have counselled people into committing suicide. The owners of the AI chatbots rightly claim this was never the intention, and it was never part of the programming. They cannot control what the user will ask the program. Even if rules such as 'do not support suicide' are included, the AI system can evolve and adapt to this, modifying the rules and its responses.

The "black box" nature of many AI models means that understanding how a system arrived at a particular decision is impossible. , complicating efforts to hold individuals or organisations accountable. This lack of transparency can hinder an individual's right to challenge outcomes that affect them. People seeking justice through legal action are frustrated because current laws may not adequately address situations in which harm arises from autonomous decision-making rather than direct human action. The AI program makes the decision, but it cannot be sued. But should the programmers, the testers, the owners be sued?

8.2 Societal Challenges

AI is fast becoming an everyday tool for many people. It is deeply embedded in social media. Most computer programs include AI assistants that can help people with tasks ranging from creating PowerPoint presentations to answering emails. University students use AI to help search for information, draft their essays, and even answer everyday questions. Yet, what does this mean for future generations? We sometimes think that not having to mess around putting pictures into PowerPoint or writing a word-for-word essay will mean a more efficient, easier life. What will it mean when people are more receptive to responses written in nice, polite AI letters rather than messages which may be ungrammatical and messy but from a human? If people can no longer find their own way to the nearest train station and rely on AI instructions, or when they are sad, chat with their AI friend to cheer them up, how will this change the nature of communities? These are critical questions to ask as AIs become more present in everyday life.

8.2.1 Ethical Decision-Making in AI

As artificial intelligence (AI) systems are increasingly used in sensitive areas such as healthcare, criminal justice, and public safety, they raise significant ethical concerns. One commonly discussed example is the use of AI in allocating scarce medical resources during emergencies, such as pandemics or natural disasters. In situations where intensive care unit (ICU) beds or ventilators are limited, AI systems may be proposed to assist in deciding which patients receive treatment. These systems often prioritise patients based on factors such as survival probability or expected life expectancy. At first glance, using AI in such decisions may appear fairer than relying solely on human judgment. Human decision-makers, even when well-intentioned, may be influenced by personal values, emotional stress, or unconscious bias. An AI system, by contrast, may seem more objective, consistent, and independent. However, this apparent neutrality is misleading. AI systems are designed by humans and trained on existing data, which may already reflect social inequalities and hidden biases.

As a result, AI systems may unintentionally favour certain groups over others—for example, prioritising younger patients over older ones, or disadvantaging individuals with disabilities, chronic illnesses, or pre-existing medical conditions. These outcomes raise serious human rights concerns, particularly in relation to the principles of equality, non-discrimination, and the right to life and health. Furthermore, difficult questions arise when AI-assisted decisions cause harm: if a patient is denied care due to an algorithmic decision, who should be held responsible, the programmer, the hospital, the healthcare provider, or the state?

Studies show that AI systems can reflect global preferences and biases when making moral decisions. A well-known example is the Moral Machine experiment conducted by MIT, which explored ethical choices in AI through versions of the "Trolley Problem." In these scenarios, a self-driving car must choose between harmful outcomes, such as saving passengers or pedestrians, or deciding between different individuals, for example, an elderly person or a pregnant woman. These dilemmas are not theoretical; autonomous vehicles may face them in real life. By analysing millions of responses from around the world, the experiment showed that moral preferences vary across cultures and that AI systems trained on this data can inherit these biases. This raises an important question: should AI be allowed to make life-and-death decisions if it reflects human bias? Or is it better to rely on imperfect human judgment, where responsibility and accountability are clearer?

One of the most contentious issues arising from AI development is the delegation of life-and-death decisions to machines through the use of Autonomous Weapons Systems (AWS). AWS is designed to select and engage targets without human intervention, raising questions about the morality of allowing machine algorithms to make life-or-death decisions. Currently, by international standards in armed conflict, or International Humanitarian Law (IHL) this is illegal. However, this may not stop some armed groups from using AI technology this way. Removing humans from the decision-making loop diminishes accountability and violates the laws of armed conflict. The laws state that the act of killing should remain a human responsibility done by soldiers, ensuring that military standards, such as the protection of certain people and places, are factored into decisions in the use of force.

This shift to AI-enabled weaponry, such as AI-based drone systems for Unmanned Aerial Vehicles (UAVs), carries significant human rights concerns. The automation of warfare could potentially lower the thresholds for initiating conflict by making military action more appealing and seemingly less costly in terms of human lives. A robot war sounds less threatening. The perception that engaging in combat is less risky without direct human involvement might lead to more frequent military interventions or pre-emptive strikes based on algorithmic assessments rather than strategic evaluations. There is also concern that AI may lead to a proliferation of risks associated with these systems; there is a profound risk that autonomous systems could be hacked or manipulated by malicious actors, leading to unintended consequences or attacks on civilian populations. The ease with which AI can be weaponised also raises fears about its proliferation among non-state actors or rogue states, potentially leading to an arms race in autonomous weaponry.

Reflection and Discussion:

- *Why does international humanitarian law require humans, not machines, to make life-and-death decisions in armed conflict? What happens to accountability when autonomous weapons are used?*
- Do you think the use of AI-enabled weapons, such as autonomous drones, makes it easier for states to go to war? How might this affect the right to life and civilian protection?

8.2.2 Human Dependency and Cognitive Erosion

Artificial intelligence (AI) increasingly shapes how people think, learn, and make decisions. As individuals rely more heavily on AI systems, new forms of human dependency emerge, raising concerns about cognitive erosion and the gradual loss of human skills. Although AI improves efficiency and enhances human capabilities, excessive dependence on these technologies may weaken individuals' ability to act independently and freely, which is closely linked to human dignity and autonomy. A clear example of this dependency appears in everyday navigation. Many people rely heavily on digital navigation tools such as Google Maps and Waze for travel. While these applications offer convenience and efficiency, heavy reliance on them can reduce a person's natural spatial awareness, such as the ability to read maps or identify basic directions like north and south. Research suggests that frequent use of GPS-based navigation is associated with reduced spatial reasoning and wayfinding skills.

In documented incidents, drivers have followed navigation instructions into dangerous situations, including instances in which vehicles were directed onto unfinished roads or bridges, resulting in serious accidents. These incidents highlight the risks of unquestioning reliance on AI systems. When users lose the ability to independently assess their surroundings or override incorrect instructions, AI errors can have life-threatening consequences. From a human rights perspective, such situations raise concerns about the rights to life and personal safety, particularly when technological failures combine with weakened human judgment. In emergency situations such as natural disasters or infrastructure collapse, these risks become even more severe. If digital systems fail due to power outages or internet disruptions, individuals who have become overly dependent on AI-based navigation may be unable to find safe routes or reach assistance, further endangering their lives.

Similar risks arise in the education sector. AI technologies increasingly support personalised learning by adapting content to individual student needs and improving efficiency. However, excessive reliance on AI tools may undermine critical thinking, independent reasoning, and deep learning. Students who rely heavily on AI to complete assignments may disengage from active learning, leading to a superficial understanding of concepts rather than genuine intellectual development. Everyday examples illustrate this shift: many people no longer memorise phone numbers, and students increasingly rely on AI to write grammatically correct sentences or summarise complex academic texts. While these tools save time and improve presentation, they may weaken essential cognitive skills such as reasoning, analysis, and synthesis. From a human rights perspective, these trends raise concerns about the right to education, which extends beyond access to learning tools and includes the development of critical thinking, intellectual independence, and personal growth. Although AI can help students produce polished and technically accurate work, it cannot replace the human capacity to question, reflect, and engage critically with knowledge.

8.2.3 Job Displacement and Economic Inequality

Artificial intelligence (AI) promises increased efficiency and productivity, but it also poses serious risks to employment and economic equality. As AI systems and automation technologies replace human labour, many traditional jobs disappear, particularly in sectors that rely on routine or repetitive tasks. Projections suggest that AI could displace up to 800 million jobs globally by 2030, making job loss one of the most significant social consequences of technological change.

The impact of automation is already visible. The widespread use of industrial robots has contributed to the loss of millions of manufacturing jobs worldwide. At the same time, large corporations increasingly announce workforce reductions as they adopt AI-driven systems to cut costs and increase efficiency. These changes do not affect all workers equally. Instead, they tend to benefit those with advanced technical skills, higher education, or access to retraining opportunities, while low-skilled and precarious workers face greater insecurity.

This uneven distribution of benefits deepens economic inequality. Workers who can adapt to AI technologies, such as engineers, data analysts, and software specialists, are more likely to experience wage growth and job mobility. In contrast, workers in low-skilled or manual occupations often struggle to transition into new roles, especially where retraining programmes are limited or inaccessible. The rapid pace of technological change further widens this skills gap, leaving many workers behind before they can adjust.

Widespread job displacement raises concerns about the rights to work, to just and favourable conditions of employment, and to an adequate standard of living. Employment is not only a source of income but also a key component of human dignity, social inclusion, and personal security. When workers lose their jobs without adequate social protection, retraining opportunities, or alternative employment, they face increased risks of poverty, marginalisation, and social exclusion.

8.2.4 Cultural and Linguistic Preservation

AI technologies are increasingly crucial in cultural preservation. They can increase the visibility of cultural assets, support digital preservation, and predict threats to heritage sites. At the same time, AI poses significant threats to the integrity, authenticity, and conservation of cultural and linguistic heritage. These problems present serious human rights concerns, particularly on cultural rights, authors' rights, Indigenous rights, and non-discrimination.

One key challenge is data presentation and interpretation. AI systems are educated on vast datasets that do not always accurately represent the diversity and complexity of global cultures. When AI models rely significantly on Western art, history, or language for training, they may fail to detect or appropriately understand symbols, themes, and techniques from non-Western cultures. This can lead to digital representations that misrepresent the significance of cultural items, alter historical narratives, or promote stereotypes. According to human rights principles, such distortion damages cultural identity and dignity while also contributing to unequal cultural recognition in digital settings.

Concerns are also raised about authenticity and control over creative works. Artificial intelligence technologies are rapidly being utilised to digitally recreate, enhance, or edit artworks for online platforms and social media. While these techniques may improve accessibility, they risk distorting the work's original flavour. An AI system that "touches up" a painting with large datasets may create a version that is drastically different from the original. When this happens without the artist's permission, it raises issues of moral rights, authorship, and consent. These problems worsen when cultural materials are updated primarily for economic gain, transforming cultural expression into a commodity owned by AI businesses rather than the producers or communities themselves.

These hazards are especially severe in the context of Indigenous art and culture. When AI systems copy, modify, or sell Indigenous artworks, cultural practices may shift from being manifestations of communal identity to objects for consumption. When access and profit are prioritised over cultural meaning, digitisation can decontextualise items. This challenge is exacerbated when Indigenous groups are barred from making decisions about how their cultural material is digitised, displayed, or repurposed. In terms of human rights, this undermines Indigenous peoples' rights to cultural self-determination and participation.

Weak legal safeguards exacerbate these issues. When regulations fail to sufficiently safeguard authors' rights or traditional knowledge, AI systems may have unlimited access to cultural materials. This may directly contradict traditional traditions that restrict access to specific information or objects depending on age, gender, or social role. Such limits are not impediments to knowledge, but rather necessary components of cultural governance. When AI disregards these boundaries, it jeopardises communities' freedom to govern and preserve their cultural legacies in accordance with their own beliefs.

AI also has complex implications for linguistic preservation. On the one hand, AI systems can help endangered languages through transcription, translation, and documentation. AI systems, on the other hand, prefer dominant global languages like English, Spanish, and Mandarin. As a result, minority and Indigenous languages remain underrepresented in digital spaces. This marginalisation restricts access to AI technologies for speakers of these languages and fosters linguistic inequality.

Language bias in AI influences how knowledge and social interactions are represented. Many AI language models incorporate elements from dominant languages, such as simplified family structures often found in English. More complicated kinship systems, such as specific distinctions between cousins on a father's or mother's side, are frequently lacking in less widely spoken languages. When these language notions disappear from digital systems, they may also fall out of common use.

The reliance on AI translation and language tools may weaken the incentive to study and use native languages, particularly among younger generations. This can eventually lead to the loss of traditional language abilities and to the interruption of intergenerational information transfer. This raises questions about linguistic rights, cultural survival, and equitable access to digital technology.

You are here: Whose Culture Is Being Shown?

You scroll through a beautifully edited image of a cultural artefact online. It looks authentic—but you wonder who decided how it should look, what story it tells, and whether the community it comes from had any say at all.

8.3 Technical Challenges

AI poses many technical challenges in ensuring equitable use and fairly distributed benefits. Responses to these challenges are crucial for ensuring the sustainable, efficient, and reliable development and deployment of AI systems. This is important in areas such as energy consumption, data quality and quantity, and accessibility to the hardware needed to run AI.

8.3.1 Energy Consumption

The energy consumption associated with operating AI models is substantial. Training large models, particularly those used in natural language processing and image generation, requires immense computational power. For example, training a model such as GPT-3 has been reported to consume electricity equivalent to the annual energy use of approximately 130 urban households. As more organisations adopt AI technologies, these high energy requirements place increasing strain on existing energy infrastructure.

Because most AI systems require large-scale computing resources, the expansion of data centres has become inevitable. These facilities must operate continuously to support the training, deployment, and real-time functioning of AI models. As a result, energy demand from AI-focused data centres is rising rapidly, with some estimates suggesting that their electricity consumption could eventually rival that of entire countries, such as Japan. This growing demand places additional pressure on local power grids, increasing the risk of power shortages during peak periods and driving up energy costs for surrounding communities.

Reflection and Discussion:

- *How does the growing energy demand of AI technologies challenge the human right to an adequate standard of living, particularly in relation to access to affordable electricity?*
- *Who benefits most from large-scale AI development, and who bears the costs when energy prices rise? Is this distribution fair from a human rights perspective?*

The situation is further worsened by the fact that much of the electricity used by data centres still comes from non-renewable energy sources. This reliance contributes significantly to greenhouse gas emissions and exacerbates climate change. Climate change, in turn, directly threatens a range of human rights, including the right to life, the right to health, and the increasingly recognised right to a healthy environment. As the World Economic Forum has noted, although AI currently accounts for only a portion of the technology sector's energy consumption, its share is expected to grow rapidly as AI adoption expands.

Another challenge linked to AI's energy use is the Jevons Paradox, the idea that improvements in efficiency can lead to increased overall consumption rather than reductions. When technologies become cheaper or more energy-efficient, they are often used more intensively, cancelling out potential environmental gains. For example, if electric taxis become cheaper and produce fewer emissions per trip, more people may choose to use taxis, ultimately increasing total energy consumption and emissions. Similarly, as organisations adopt more energy-efficient AI systems, lower operational costs may encourage greater and more frequent use of AI, increasing overall energy demand.

This dynamic can undermine efforts to reduce carbon emissions and slow progress toward net-zero targets needed to address climate change. If AI-driven development contributes to environmental harm, the resulting impacts, such as extreme weather, resource scarcity, and displacement, are disproportionately borne by vulnerable communities.

8.3.2 Data Quality and Quantity

Data quality refers to the accuracy, completeness, consistency, and reliability of data. High-quality data is essential for effective AI model training and deployment. However, many organisations struggle with poor data quality due to several factors such as inconsistent data sources and inadequate data pre-processing procedures. Inconsistent data can be observed when organisations often collect data from multiple sources. For example, if information on a person is recorded differently across various databases, it may lead to discrepancies that impact AI outputs. An example of this is the infamous 'robodebt' scheme used in Australia to check if recipients of social security were cheating the system. By comparing the tax office database (based on yearly earnings) with the social security database (based on fortnightly earnings), the program created debts that did not exist. Often these debts were forced on people using social welfare, who had little financial resources to challenge these claims. In some cases, people committed suicide fearing they could never repay a debt, which they did not actually owe. If an AI model is trained on inconsistent data, it may produce unreliable predictions or insights such as this. This impact underscores the necessity for governments and businesses to prioritise data quality management as they adopt AI technologies. If data is not accurately and fairly processed, sometimes called data cleaning processes, the result is the retention of "bad data" which may include duplicates, inaccuracies, or irrelevant information that can skew AI model outcomes. Although AI can automate some aspects of data cleaning, if the initial dataset is flawed, even advanced algorithms will struggle to produce meaningful results.

Another issue is when datasets grow and age. Based on the Diminishing Returns concept, as datasets grow larger, the incremental value gained from additional data diminishes. This phenomenon can lead organisations to over-invest in data collection without achieving improvements in model performance. After a certain point, adding more data does not significantly improve predictive accuracy and may even introduce noise that complicates analysis. For instance, a government might collect vast amounts of health data in the hope of improving its services and recommendations. However, if the additional data contains irrelevant or low-quality interactions, they could degrade the model's performance rather than enhance it.

Poor data quality is not just a technical failure but a governance failure with real consequences for people's lives. When AI systems rely on inaccurate, inconsistent, or outdated data, they can produce unfair and harmful decisions that affect access to social security, healthcare, employment, and other essential services. These errors disproportionately harm vulnerable groups who often lack the resources to challenge automated outcomes, raising concerns about the rights to equality, dignity, due process, and effective remedy.

8.3.3 Hardware Limitations

AI increasingly relies on specialised hardware to perform complex computations that will process vast amounts of data. AI algorithms must use high-performance hardware, such as Graphics Processing Units (GPUs) or specialised AI chips. Despite advancements in chip technology, many current AI models demand more computational resources than what existing hardware can provide. For instance, leading-edge models can have hundreds of billions of parameters, requiring massive computational resources for training and inference. The previous assumption, as outlined in Moore's Law, says that processing power roughly doubles every two years. Historically, advancements in semiconductor technology has followed Moore's Law, but now this trend is slowing down as physical limitations are reached in chip manufacturing. As a result, the pace of improvement in processing power is not keeping up with the growing demands of advanced AI models. The inability to scale processing power effectively slows innovation and limits the potential applications of AI technologies.

Another technical issue is the "Memory Wall" problem, where it is quicker to process information than to access it because CPU performance is faster than and memory access speeds. For instance, accessing memory off-chip consumes up to 200 times more, energy than performing computations on-chip, leading to inefficiencies in processing.

These technical limitations are a problem for the technology industry to solve through developing hardware abilities. In addition, there are political concerns given that the majority of the best processors are made in a small number of countries, and can be very expensive. This makes access to these chips not only an economic concern, but also a political one. Corporations and States can make decisions about who they sell these chips to. Sometimes called the 'Chip War,' countries such as the USA have tried to limit China's access to high end chips. Further, poorer countries are unable to compete in this market because their digital infrastructure does not have the resources of money to use high-end chips, which may cost over ten thousand dollars for a single chip, and some AI programs need many chips to function.

AI does not work by magic, it needs very powerful and very expensive computer chips. Only a few countries and companies make these advanced chips, and not everyone can afford them. This means that some countries and large corporations get to use and benefit from advanced AI, while others are left out. When access to technology depends on money and political power, AI can end up increasing global inequality instead of reducing it. This raises important questions about fairness, equal access to technology, and who gets to shape the future of AI.

Reflection and Discussion:

- *Is it fair that only wealthy countries and corporations can afford the hardware needed to develop advanced AI? Why or why not?*
- *How does control over AI chips give certain states or companies more power? What human rights concerns does this create?*

8.3.4 Intellectual Property Rights in the Age of Generative AI

Generative AI has led to conflicts over intellectual property law, including copyright, patents, and trademarks. One of the primary challenges is determining who qualifies as the author of a work generated by an AI system. Traditionally, copyright law attributes authorship to human creators. However, when an AI autonomously generates art, music, or literature, questions arise: who owns the copyright? Is it the programmer who created the AI, the user who provided the prompts, or should the work receive no copyright protection at all?

Several legal cases have begun to address these questions. In some rulings, courts have held that human involvement is necessary for copyright protection. This suggests that purely AI-generated works may not qualify. In other situations, courts have recognised that human input in guiding AI processes can establish originality, particularly where prompts, selection, and arrangement by a human user shape the final output.

The issue of data scraping further complicates intellectual property rights. Generative AI systems are often trained on vast datasets that include copyrighted materials taken from the internet without proper authorisation or licensing. This practice raises serious concerns about copyright infringement. A notable example is Getty Images' accusation that Stability AI used millions of images from its database without permission or compensation. This case highlights the lack of clear rules on data use in AI training and the uncertainty around liability when copyrighted content is reproduced. The absence of clear accountability also raises concerns about who is responsible when AI systems generate infringing content or spread misinformation.

These issues affect creators' rights to recognition, fair compensation, and control over their work. When AI systems use creative content without consent or payment, they risk undermining artists' and authors' livelihoods and dignity. At the same time, unclear ownership and accountability make it difficult for affected individuals to seek remedies when harm occurs, raising concerns about fairness and access to justice in the digital economy.

8.4 Towards a Just and Equitable Digital Future: A Shared Responsibility

Artificial Intelligence (AI) presents humanity with a pivotal challenge: to steer digital advancement towards a future that is not only innovative but also inherently just and equitable. This section reviews key elements to include in developing social, legal, and political responses to AI.

8.4.1 The Imperative for Adaptive, Inclusive, and Globally Coordinated Governance

AI poses challenges for traditional legislative and governance frameworks, often creating a "governance gap" in which laws designed for stability struggle to keep pace with rapidly evolving issues such as AI, big data, and blockchain. Unless this gap is addressed, there may be innovations developed without adequate safeguards that increase the potential for misuse, harm, and human rights violations..

Governance has to evolve to ensure an adaptive, inclusive, and globally coordinated response. A demanding criterion is that laws be flexible enough to adapt to emerging technologies, which is difficult because it often takes years to write, legislate, and implement a law, while new technologies can emerge in months. For instance, while the European Union's proposed AI Act attempts to categorise AI systems by risk levels, early drafts have struggled to encompass emerging technologies such as large language models and generative AI. Laws could be implemented to control what AI can do, though technology companies may dislike the idea that research or innovation in some areas becomes illegal. Laws could increase the sanctions for destructive technologies. Though, again, technology companies may find it unfair to be held responsible for how people use their products. We don't fine car manufacturers if someone crashes their car.

International cooperation and the development of binding international standards may help to ensure AI technologies are governed by the same rules no matter where they are developed or used. This is important to address cross-border issues like global data flows, prevent the "race to the bottom" where companies exploit weaker regulations in certain jurisdictions, and establish consistent standards across diverse legal systems. Developing this international system requires bridging gaps in technical expertise between the rich and poor countries, between public institutions and civil society organisations, and between technology giants and small businesses, to tackle complex digital rights issues such as data privacy, cybersecurity, and algorithmic bias.

8.4.2 Empowering Individuals and Communities

A just and equitable digital future depends on empowering individuals and communities to understand, navigate, and shape the digital world. This includes ensuring digital literacy, fostering meaningful participation, and promoting inclusive technology design.

Digital literacy initiatives equip individuals with the skills to effectively find, evaluate, communicate information, understand the implications of data usage, and advocate for their rights. It is beneficial for marginalized and vulnerable groups who often have lower literacy and limited digital access, hindering their ability to benefit from digital advancements or engage meaningfully with technology.

Meaningful participation ensures that individuals and communities have opportunities to voice their concerns and influence how technologies are developed and governed. Based on fostering democratic and equitable processes, this involves inclusion of all people in decisions about data governance and digital inclusion programs. For instance, Thailand's FireD application, which allows citizens to report forest fires and open burning, demonstrates how digital technology can strengthen citizen participation in public affairs and narrow the rural-urban information gap through inclusive, community-driven action.

Finally, inclusive technology design, often guided by Human-Centred Design (HCD) principles, places human needs, values, and experiences at the heart of system development. HCD should make AI systems usable by individuals with diverse physical, cognitive, socio-economic, and linguistic abilities, ensuring no group, particularly marginalised or vulnerable populations, is left behind. This approach supports the goal of ensuring that everyone, regardless of socioeconomic status or physical ability, can benefit from technological advancements.

8.4.3 Evolving Human Rights Law for the Digital Age

AI tests the limits of human rights standards. State obligations need to be refigured, as do duties and obligations of companies, individuals, and protected groups. States, as primary duty-bearers, have legal obligations to protect human rights, which, in the digital age, translate into duties to ensure rights such as digital access to education, media, healthcare, and other information services. Almost every government service, from a passport to paying tax, needs access to the internet. Laws must recognise that access to technology is a human right. This also includes protecting people from violations in the digital arena, whether these are bullying of children, invasions of privacy, or the theft of people's property through scams and data breaches.

Non-state actors, particularly technology companies, wield significant power over digital ecosystems and must be held accountable for their impacts on human rights. The UN Guiding Principles on Business and Human Rights (UNGPs) framework for corporate responsibility emphasises that businesses must respect human rights, avoid adverse impacts, and provide access to remedy. This requires companies to conduct human rights due diligence, be transparent about the development and use of their technology, and establish accessible grievance mechanisms. However, the voluntary nature of the UNGPs can limit their enforcement and accountability. The evolving legal landscape also includes rights like the "right to be forgotten," which allows individuals to request the removal of irrelevant personal information, balancing individual rights with economic interests and public access to information.

8.4.4 Multi-stakeholder Collaboration for Responsible Innovation in Southeast Asia

A just and equitable digital future in a diverse region like Southeast Asia is a multi-stakeholder obligation. Governments, businesses, civil society organisations, and educational institutions have interrelated rights and duties. Governments are responsible for integrating human rights into policy-making, legislation, and developing digital infrastructure. Regional initiatives like the ASEAN AI Guide, the ASEAN Data Management Framework, and the ASEAN Digital Economy Framework Agreement (DEFA) aim to promote inclusive growth and ethical governance. However, their non-binding nature and varying commitments to human rights across member states substantially weaken these standards.

The private sector plays a crucial role in innovation and investment. But this must be done within the law. They should conduct human rights due diligence and ensure transparency in their operations. But again, given their non-binding nature, it is unfortunately common to see these companies minimise their human rights obligations or outsource violations to the end user. For example, hate speech circulating on social media platforms is often blamed on the people who upload it, rather than blaming the platform for allowing the distribution of it.

Civil society organisations (CSOs) can be watchdogs, advocates, and educators. They monitor the impact of technology on human rights, scrutinise state and corporate practices, advocate for stronger regulations, and empower communities with digital literacy skills. They may be one of the few groups to hold governments and corporations accountable and amplify the voices of marginalised communities.

Educational institutions also contribute by preparing individuals to address the human rights challenges posed by technology, integrating human rights into curricula, conducting relevant research, and fostering dialogue among stakeholders.

Ideally, these stakeholders should work together towards a transformational technological justice. AI is still in the early stages of development, and legal and social responses are varied in their ability to ensure justice. New problems and concerns arise regularly. Turning off AI is no longer an option. Still, the fundamental principles of human rights, such as participation, inclusion, and justice, remain relevant in developing responses to it.

You Are Here: Governance Is Not Distant from You

Decisions about AI governance affect how safely you learn, work, communicate, and exist online. Whether technology becomes empowering or harmful depends not only on innovation, but on whose voices are heard when rules are made.

8.5 Conclusion

This chapter has shown that governing emerging technologies is not simply a matter of creating better rules or keeping pace with innovation. The challenges are deeper and more structural. Rapid technological change, opaque decision-making systems, growing human dependence on automation, environmental costs, and fragmented responsibility all make effective governance difficult, especially when harm occurs before safeguards are in place. Across these challenges, a common pattern emerges: technology often advances faster than our ability to understand, regulate, or hold it accountable. “Black box” systems undermine transparency, data errors produce real and unequal harms, and the benefits of innovation are frequently enjoyed by a few while risks are distributed more widely. In Southeast Asia, these problems are further complicated by regulatory gaps, capacity constraints, and the limits of regional coordination.

Rather than offering simple solutions, this chapter highlights the importance of asking the right questions. Who benefits from emerging technologies, and who bears their costs? Who has the power to design, deploy, and profit from these systems, and who is left to deal with their consequences? Without clear answers to these questions, governance risks becoming reactive, fragmented, and ineffective. Ultimately, the future of emerging technologies will be shaped not only by engineers and policymakers, but also by how societies respond to these challenges. As users, students, and future professionals, readers have a role in questioning unchecked innovation, demanding transparency and accountability, and recognising that technological progress should not come at the expense of human rights. Governing emerging technologies is difficult, but ignoring these challenges makes the risks far greater.

Key Takeaways

1. Rapid technological innovation outpaces the slow response of legislative bodies, creating a “governance gap” that increases the risk of misuse and human rights violations because safeguards are deployed too late.
2. The complexity and “black box” nature of many AI systems make it difficult to understand how they arrive at decisions, complicating the accountability and liability when harm occurs.
3. Multinational technology corporations wield enormous power over digital ecosystems, and their reliance on voluntary adherence to human rights frameworks limits enforcement and accountability.
4. There are dilemmas in AI used in critical areas like healthcare resource allocation. . Ensuring that AI decisions align with societal values is challenging, and biased data can lead to discrimination.
5. Reliance on technologies, such as navigation systems, can diminish critical human skills and overall human agency, a phenomenon known as cognitive erosion.
6. AI models trained on non-diverse data can perpetuate stereotypes, distort historical narratives, and risk accelerating the erosion of minority languages that lack digital support.
7. Human rights law must evolve to address new digital challenges, including clarifying state duties and regulating powerful non-state actors (tech companies).
8. Achieving a just digital future demands a shared responsibility, requiring adaptive, globally coordinated governance, and empowering communities through digital literacy and meaningful participation

Issues to Think About

- If an AI system acts as a “black box” and causes harm, making its decision-making invisible, how can legal systems accurately decide who is responsible (the user, the programmer, or the company)?
- Since large multinational technology corporations often follow human rights rules voluntarily, how can governments create strong, binding regulations to prevent these companies from prioritizing profit over people’s rights?
- Should limits be made to the energy consumption required to train and run large AI models?
- If an AI system is used in an emergency to make ethical trade-offs, like deciding who gets critical care resources, is this ‘objective’ decision process better than using a human?

Further Readings

ASEAN Universities Network. (2024). *Driving the digital transformation and impacts of ASEAN higher education through partnerships*. https://www.aunsec.org/news/driving-digital-transformation-and-impacts-asean-higher-education-through-partnerships

Barrett, A. M., Hendrycks, D., Newman, J., & Nonnecke, B. (2022). Actionable guidance for high-consequence AI risk management: Towards standards addressing AI catastrophic risks [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2206.08966

Federal Bar Association. (2025). *The legal industry report 2025*. https://www.fedbar.org/blog/the-legal-industry-report-2025/

Foley, A., & Melese, F., (2025). *Disabling AI: Power, exclusion, and disability*. https://www.tandfonline.com/doi/full/10.1080/01425692.2025.2519482

JD Supra. (2025). *AI watch: Global regulatory tracker - United Nations (UPDATED)*. https://www.jdsupra.com/legalnews/ai-watch-global-regulatory-tracker-9050110/

Kumar, S., & Choudhury, S. (2022). Normative ethics, human rights, and artificial intelligence. *AI and Ethics*, 3(2), 441-450. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4066393

Mpinga, E. K., Bukonda, N. K., Qailouli, S., & Chastonay, P. (2022). Artificial intelligence and human rights: Are there signs of an emerging discipline? A systematic review. *Journal of Multidisciplinary Healthcare*, 15, 235-246. https://pmc.ncbi.nlm.nih.gov/articles/PMC8819698/

National Conference of State Legislatures. (2025). *Summary of artificial intelligence 2025 legislation*. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation

Roberts, H., Cowls, J., Hine, E., Morley, J., Wang, V., Taddeo, M., & Floridi, L. (2023). Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. *The Information Society*, 39(2), 79-97. https://www.tandfonline.com/doi/full/10.1080/01972243.2022.2124565

Roberts, T., & Oosterom, M. (2024). Digital authoritarianism: A systematic literature review. *Information Technology for Development*. 1-25. https://www.tandfonline.com/doi/full/10.1080/02681102.2024.2425352

U.S. Copyright Office. (2025). *Copyright and artificial intelligence, Part 2: Copyrightability report*. https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf

UNESCO. (2025). *Safeguarding human rights and judicial independence in the age of algorithmic justice*. https://www.unesco.org/en/articles/safeguarding-human-rights-and-judicial-independence-age-algorithmic-justice

United Nations General Assembly. (2023). *Report of the Office of the UN High Commissioner for Human Rights: Human rights and technical standard-setting processes for new and emerging digital technologies*. (A/HRC/53/42). https://docs.un.org/en/A/HRC/53/42

About ASEAN University Network - Human Rights Education (AUN-HRE)

ASEAN University Network
Human Rights Education (AUN-HRE)

Recognizing that respect for human rights and fundamental freedoms is one of the key principles for ASEAN Community building, the ASEAN University Network - Human Rights Education (AUN-HRE) was established by the ASEAN University Network Board of Trustees in 2009 with the objective of building a culture of human rights and peace in the region. The specific objectives of AUN-HRE are:

* To further efforts by different bodies in promoting human rights and peace education in ASEAN/SEA;
* To mainstream human rights and peace education envisioned by ASEAN Vision 2025 and to support the realization of SDGs (4.7);
* To strengthen capacities of lecturers/ students on research and education;
* To provide platform for exchange and collaboration within and beyond SEA region; and
* To develop materials and human resources for human rights and peace education.

With these objectives AUN-HRE has been organising: training workshops for lecturers at regional and national levels; essay competitions amongst undergraduate students in the region; and colloquiums on issues of interest expressed by its network members. It has also been producing textbooks and teaching manuals on human rights and peace.

AUN-HRE has 30 members and 2 associate members. The secretariat of AUN-HRE is hosted by the Institute of Human Rights and Peace Studies at Mahidol University in Thailand.

AUN-HRE Secretariat
Institute of Human Rights and Peace Studies, Mahidol University
Panyaphiphat Building
999 Phuttamonthon 4 Rd., Salaya
Nakhon Pathom 73170, Thailand

Tel : (66) 2-441-0813-5
Fax : (66) 2-441-0872-3
E-mail: aunhre.secretariat@gmail.com
Website:http://www.ihrp.mahidol.ac.th/

About the Institute of Human Rights and Peace Studies (IHRP), Mahidol University

Institute of Human Rights
and Peace Studies
Mahidol University

The Institute of Human Rights and Peace Studies (IHRP) was established in 2011 by the merging of two centres at the Mahidol University: Center for Human Rights Studies and Social Development and Research Center for Peacebuilding.

The Center for Human Rights Studies and Social Development (CHRSD) was established in 1998. For more than ten years, it served as an academic institution specialized in human rights, with a track record in providing postgraduate education as well as training programs to students, human rights workers, human rights defenders, members of civil society organizations and government

officials. The MA in Human Rights started by the CHRSD is the longest running graduate degree program in Human Rights in Asia.

The Research Center for Peacebuilding was founded in November 2004 as a research center with the impetus to be part of the peaceful solution to conflicts in Thailand especially the conflict in three southernmost provinces: Pattani, Yala, and Narathiwat. The Center developed and implemented considerable action and participatory research projects. These projects focussed on facilitating cooperative efforts to deal with the conflicts through opening space for dialogue at all levels and identifying needs of community and society. Also, the projects provided inputs to policy makers on transforming conflicts and building just and peaceful societies.

Combining the experience and perspective of both these centres, IHRP is uniquely interdisciplinary in its approach and is committed to the advancement of human rights and peace by: educating human rights and peace practitioners; promoting outreach programs to community and international organizations; and conducting cutting edge research on important issues. The four academic programs implemented by it are:

1. Ph.D Human Rights and Peace Studies (International Program)
2. M.A. Human Rights (International Program)
3. M.A. Human Rights and Democratisation (International Program)
4. M.A. Human Rights and Peace Studies (Thai Program)

IHRP also hosts the secretariat of ASEAN University Network - Human Rights Education (AUN-HRE) and Strengthening Human Rights and Peace Research and Education in ASEAN / Southeast Asia (SHAPE-SEA).

Institute of Human Rights and Peace Studies, Mahidol University

Panyaphiphat Building, 999 Phuttamonthon 4 Rd., Salaya
Nakhon Pathom 73170, Thailand

Tel : (66) 2-441-0813-5
Fax : (66) 2-441-0872-3
Website:http://www.ihrp.mahidol.ac.th/

About Norwegian Centre for Human Rights (NCHR), University of Oslo

UiO : Norwegian Centre for Human Rights
University of Oslo

The Norwegian Centre for Human Rights (NCHR) is a multi- and interdisciplinary centre. Through research, teaching, and dissemination, the Centre shall promote the subject of human rights as an academic field, and strengthen its international position as a central actor and attractive collaborative partner within the human rights field. The NCHR emphasizes the connection between research, education, and practical application, among other things through international projects and programmes.

Website:
https://www.jus.uio.no/smr/english/about/