PERADI
PERHIMPUNAN ADVOKAT INDONESIA
INDONESIAN ADVOCATES ASSOCIATION

36th POLA SUMMIT
CRIMINAL LAW IN TRANSITION:
"INDONESIA'S NEW CODE AND GLOBAL PERSPECTIVES"
6 – 8 September 2026, Pullman Hotel - Jakarta, Indonesia

Addressing Cybercrime & Emerging Offences in the Digital Age

Anand Raj
President, Malaysian Bar

What is "*Cybercrime*"?

- There is no universally accepted definition of cybercrime.
- **United Nations Office on Drugs and Crime**: "*Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime*".
- **United Nations Convention on Cybercrime** define cybercrime via list of emerging offences ICT systems which include:-

1. Illegal access
2. Illegal interception
3. Interference with electronic data
4. Interference with an ICT system
5. Misuse of devices
6. ICT system-related forgery
7. ICT system related theft or fraud
8. Online child sexual abuse or child sexual exploitation material
9. Solicitation or grooming for the purpose of committing a sexual offence against a child
10. Non-consensual dissemination of intimate images

Recognised "Cybercrime" offences under International Law

Scope of Cybercrime Law

What SHOULD be covered

- Cyber offences: Illegal access (hacking), illegal interception of data, system or data interference and device/ malware misuse
- ICT crimes: Forgery and online financial fraud
- Child exploitation: Production, distribution and possession of online child sexual abuse and exploitation material and online grooming
- Content based harms: Non-consensual dissemination of intimate images
- Associated acts: Money laundering tied to cyber operations

What should NOT be covered

- No infringement of any constitutional rights
- No warrantless search and seizures
- No unauthorised surveillance
- No disproportionate state overreach
- No criminalisation of legitimate free speech or journalism

Protection of Human Rights

UN Convention Against Cybercrime [2024]

Article 6: Respect for human rights

- State Parties must implement obligations under the Convention in a manner consistent with international human rights law.
- Nothing in the Convention allows for the restriction of human rights or basic freedoms such as speech, belief, religion and assembly as protected by international law.

Article 24: Conditions and safeguards

- Each State Party must ensure that powers and procedures include strong human rights safeguards based on the principle of proportionality and subject to *independent judicial oversight* both domestically and when assisting other nations.

Convention on Cybercrime (Budapest Convention) [2001]

Article 15: Conditions and safeguards

- Every participating country must create domestic legal protections and safeguards.
- Laws must protect human rights especially those under international treaties like the International Covenant on Civil and Political Rights (ICCPR) and ensure all actions are strictly necessary based on the principle of *proportionality*.

Reality of Cyber Incidents

88%

Of cyber incidents in 2026 involve human error

Source: Viking Cloud

Takeaway: Since 88% of cyber incidents involve human error, effective risk mitigation requires prioritising education, awareness and continuous training.

Conclusion

"Framing privacy and other ***human rights*** as antithetical to public safety and national security is not only misleading, but undermines public safety and security, as well as freedom. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset this trend."

- Freedom Online Coalition Statement on a Human Rights Based Approach to Cybersecurity Policy Making (Internet Governance Forum (IGF) Best Practices Forum, 2018) convened by the United Nations Internet Governance Forum Secretariat

THANK YOU


BADAN PEGUAM MALAYSIA
KEADILAN MELALUI UNDANG2
JUSTICE THROUGH LAW
MALAYSIAN BAR