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 and Emerging Offences in the Digital Age

Legal frameworks, cross-border enforcement, and the protection of rights

Presented by

Allan G. Panolong
President, Integrated Bar of the Philippines

36th POLA Conference
Jakarta, Indonesia | 8 September 2026



Why This Issue Matters

- Digital systems support nearly every sector of society.
- Criminal activity can be conducted remotely and anonymously.
- One incident can affect thousands or millions of victims.
- Evidence may be stored across several countries.
- Criminal methods evolve faster than legislation.
- Victims often face financial, psychological, and reputational harm.

Core point: digital harm can quickly become institutional, economic, and human harm.

Understanding Cybercrime

Cyber-dependent crime

Crimes that require digital technology to be committed:

- Unauthorised access
- Malware and ransomware
- Distributed denial-of-service attacks
- Data interference
- System interference
- Botnet operations

Cyber-enabled crime

Traditional crimes amplified by digital technology:

- Fraud and financial scams
- Extortion
- Identity theft
- Money laundering
- Human trafficking
- Child exploitation
- Defamation and harassment

Legal systems must address both the technology itself and the underlying criminal conduct.

The Changing Threat Landscape

- Ransomware-as-a-service
- Phishing and business email compromise
- Online investment and romance scams
- Digital identity theft
- Deepfakes and synthetic media
- Cryptocurrency-related crime
- Attacks on critical infrastructure
- Artificial intelligence-assisted fraud
- Online child exploitation
- Cyber espionage and politically motivated attacks

The question is how society can manage technological risks while preserving legitimate innovation.

Emerging Offences in the Digital Age

Examples

- Non-consensual intimate image distribution
- Deepfake sexual abuse material
- Digital stalking and coercive control
- Doxxing and malicious exposure of personal information
- Coordinated online harassment
- Election and information-system interference
- AI-generated impersonation
- Digital extortion
- Unlawful biometric-data exploitation
- Manipulation of automated or intelligent systems

Key question: how can the law protect victims without overcriminalizing legitimate speech, journalism, research, or criticism?

The Main Legal Challenges

- Criminal conduct crosses national borders.
- Offenders may conceal their identity and location.
- Data can be rapidly deleted, encrypted, or altered.
- Electronic evidence is highly volatile.
- Jurisdiction is difficult to establish.
- Definitions differ between legal systems.
- Law-enforcement powers may conflict with privacy rights.
- Technology companies may operate under different legal obligations.
- Investigators require specialized skills and resources.

Strengthening National Legal Frameworks

Effective legislation should provide:

1. Clear definitions of prohibited conduct.
2. Proportionate penalties.
3. Rules for preservation and admissibility of electronic evidence.
4. Properly supervised investigative powers.
5. Protection for victims and witnesses.
6. Clearly defined corporate and intermediary responsibilities.
7. Mechanisms for rapid response to serious threats.
8. Safeguards against misuse and overcriminalization.

Philippine Cybercrime-Related Laws

- RA 10175 — Cybercrime Prevention Act of 2012
- RA 10173 — Data Privacy Act of 2012
- RA 8792 — Electronic Commerce Act of 2000
- RA 4200 — Anti-Wiretapping Act
- RA 9995 — Anti-Photo and Video Voyeurism Act of 2009
- RA 9775 — Anti-Child Pornography Act of 2009
- RA 11930 — Anti-OSAEC and Anti-CSAEM Act
- RA 8484, as amended by RA 11449 — Access Devices Regulation Act

These laws operate together: offences, evidence, privacy, child protection, online exploitation, and financial-device misuse.

Selected Philippine Cybercrime and Cyberattack Incidents

- 2000 — ILOVEYOU / Love Bug worm: e-mail malware traced to the Philippines spread globally and exposed gaps in cybercrime legislation. [1]
- 2016 — COMELEC data breach ("Comeleak"): voter records were compromised; the NPC found Data Privacy Act violations and recommended prosecution. [2]
- 2019 — DFA passport data issue: the NPC investigated claims of contractor-related non-availability of passport data; DFA later said data remained under its control. [3]
- 2021 — DFA Online Passport Tracker: DFA disabled the tracker after a data privacy issue and coordinated with the NPC. [4]
- 2023 — PhilHealth Medusa ransomware: online systems were affected; the NPC later launched a portal for people to check if their data appeared in leaked datasets. [5]

Electronic Evidence and Digital Investigations

Key principles

- Legality of collection
- Authenticity
- Integrity
- Reliability
- Chain of custody
- Reproducibility
- Secure preservation
- Proportionality of search and seizure

Practical concerns

- Cloud-based evidence
- Encrypted communications
- Multiple devices and accounts
- Metadata and log files
- Deleted or altered content
- Remote searches
- Evidence held by private platforms

Cross-Border Cooperation

- Timely preservation requests
- Mutual legal assistance
- Extradition mechanisms
- Joint investigations
- Direct cooperation with service providers
- Shared investigative standards
- 24/7 contact points
- Training and technical assistance
- Respect for sovereignty and due process

Human Rights and the Rule of Law

Cybercrime enforcement must respect:

- Legality
- Necessity
- Proportionality
- Privacy
- Freedom of expression
- Due process
- Equality before the law
- Presumption of innocence
- Access to an effective remedy

Security and liberty are not opposing objectives.
Legitimate security depends on the rule of law.



The Role of Technology Companies

- Security by design
- Privacy by design
- Transparent terms and policies
- Rapid response to abuse
- Preservation of relevant evidence
- Protection of user data
- Clear reporting mechanisms
- Cooperation with lawful investigations
- Independent auditing and accountability

Artificial Intelligence: Risk and Opportunity

Risks

- Automated phishing and fraud
- Deepfake impersonation
- Automated vulnerability exploitation
- Mass surveillance
- Bias in automated decision-making
- Fabricated evidence
- Unclear attribution and responsibility

Opportunities

- Threat detection
- Fraud prevention
- Digital forensics
- Translation and investigative cooperation
- Victim support
- Identification of criminal networks
- Legal and regulatory compliance

Protecting Victims

- Accessible reporting channels
- Rapid removal or containment of harmful content
- Protection from retaliation
- Financial recovery mechanisms
- Psychological and social support
- Privacy protection
- Legal assistance
- Cross-border referral systems
- Special safeguards for children and vulnerable persons

The Role of Bar Associations

- Promote continuing legal education on cybercrime.
- Develop model policies and legislative recommendations.
- Support specialist cybercrime and digital-evidence committees.
- Facilitate regional cooperation among lawyers.
- Provide legal assistance to victims.
- Protect due process and human rights.
- Engage with lawmakers, regulators, and technology companies.
- Encourage ethical and secure use of legal technology.
- Support lawyers facing cyber threats.

A Regional Action Framework

1. Harmonise core legal concepts

Develop common approaches to serious cyber-dependent and cyber-enabled offences.

2. Accelerate lawful cooperation

Improve preservation, mutual assistance, extradition, and institutional contact points.

3. Build capacity

Invest in prosecutors, judges, lawyers, investigators, forensic specialists, and victim-support services.

4. Protect rights

Require necessity, proportionality, oversight, transparency, and remedies.

5. Prepare for emerging technologies

Establish adaptable frameworks for AI, digital identity, cryptocurrencies, and connected devices.

Practical Recommendations

For governments

- Review cybercrime legislation regularly.
- Establish specialized investigative and prosecutorial units.
- Strengthen critical infrastructure protection.
- Improve international cooperation procedures.
- Invest in public awareness and victim support.

For courts and prosecutors

- Develop digital-evidence expertise.
- Use independent technical experts where necessary.
- Protect the integrity of proceedings.
- Apply investigative powers proportionately.

For lawyers and bar associations

- Provide cybersecurity training.
- Maintain secure client-data practices.
- Develop referral networks.
- Participate in law reform.
- Defend rights in digital investigations and prosecutions.

For the public and private sectors

- Share threat information responsibly.
- Establish incident-response plans.
- Report attacks promptly.
- Adopt security and privacy by design.

Discussion Questions

1. How can legal systems respond quickly without weakening due process?
2. What minimum cybercrime concepts should be harmonised across Asia-Pacific jurisdictions?
3. How should responsibility be allocated among users, platforms, and technology developers?
4. What safeguards are necessary for cross-border access to electronic evidence?
5. How can bar associations assist victims and improve legal capacity?
6. How should courts evaluate AI-generated or AI-assisted evidence?



Conclusion

- Cybercrime is a regional and global rule-of-law challenge.
- Technology changes faster than traditional legal systems.
- Effective laws must be clear, adaptable, and rights-respecting.
- Cross-border cooperation must be both rapid and lawful.
- Victims must remain at the centre of the response.
- Bar associations have an essential role in shaping policy and protecting justice.

"The digital age does not diminish the importance of the rule of law. It makes the rule of law more important than ever."