

Unit IX: Legal, Ethical and Professional issues in Information Security

- Relevant Laws
- International Laws and Legal Bodies
- Related laws in Nepal, their provisions and limitations.
- Ethical Concepts in Information Security
- Codes of Ethics, Certifications, and Professional Organizations

1. Relevant Laws and Legal Bodies

Cybersecurity law operates at two levels: **International**, to handle the borderless nature of the internet, and **National**, to enforce local justice.

International Laws and Legal Bodies

- **Budapest Convention on Cybercrime:** The most significant international treaty. It harmonizes national laws so that a hacker in one country can be prosecuted for a crime committed in another. It focuses on:
 - **Offenses:** Hacking, data interference, and system interference.
 - **Procedural Powers:** Search and seizure of stored computer data.
- **GDPR (General Data Protection Regulation):** Though an EU law, it has a "global reach." Any company worldwide that handles data of EU citizens must comply, making it the de facto international standard for data privacy.
- **WIPO (World Intellectual Property Organization):** A UN agency that protects digital intellectual property (IP), such as software code and digital content, across borders.

2. Related Laws in Nepal

Nepal's legal framework for the digital age is primarily anchored by two major acts.

A. Electronic Transactions Act (ETA), 2063 (2006)

This is the "Cyber Law" of Nepal. It was originally created to provide legal validity to electronic signatures but has become the primary tool for prosecuting cybercrimes.

- **Key Provisions:**
 - **Section 44:** Prohibits hacking and unauthorized access to computer systems.
 - **Section 47:** Criminalizes the publication of illegal or obscene materials in electronic form (the most frequently used and debated section).
 - **Punishments:** Fines ranging from **NPR 50,000 to 3,00,000** and/or imprisonment from **6 months to 3 years**.

1. Limitations of the Electronic Transactions Act (ETA), 2063

The ETA was designed in 2006 to handle "Electronic Commerce," yet it is currently the primary law used to prosecute hackers and social media users. This mismatch creates several issues:

- **Vague Definitions (The "Section 47" Problem):** Section 47 prohibits publishing material that is "contrary to public morality" or "spreads hate." Because "morality" isn't technically defined, this section is frequently criticized for being used to arrest journalists and citizens for simple online criticism or satire.
- **Centralization of Justice:** By law, cybercrime cases should be heard by a specialized **IT Tribunal**. However, for years, the government has failed to fully functionalize this tribunal. Consequently, almost all cybercrime cases are handled by the **Kathmandu District Court**, forcing victims from all over Nepal to travel to the capital for legal hearings.
- **Lack of Technical Expertise:** Many judges and lawyers lack specialized training in digital forensics. This can lead to cases being dismissed due to poor evidence handling or, worse, innocent people being convicted because a judge didn't understand how "IP spoofing" works.
- **No Extradition for Cyber-Criminals:** Nepal lacks specific bilateral treaties to extradite cyber-criminals. If a hacker attacks a Nepali bank from another country, the ETA 2063 is virtually powerless to bring them to justice.

B. Individual Privacy Act, 2075 (2018)

Enacted to align with the Right to Privacy guaranteed by the Constitution of Nepal.

- **Provisions:** Restricts the collection, storage, or analysis of personal data without the individual's consent. It classifies information like caste, religion, and biometrics as "sensitive."
- **Limitations:** While the law exists, the technical infrastructure to monitor data compliance in private companies is still in its infancy.

2. Limitations of the Individual Privacy Act, 2075

While this act was a massive step forward for human rights, it has significant "implementation gaps."

- **Missing Regulatory Body:** Unlike the EU (which has Data Protection Authorities), Nepal does not have a dedicated "Privacy Commission." If a company leaks your data, there is no specific technical body to investigate how it happened.
- **Offshore Entity Loophole:** The law is unclear about how it applies to foreign companies like Facebook, Google, or TikTok. If a global platform violates the privacy of a Nepali citizen, the government struggles to enforce penalties on a company that has no physical office in Nepal.

- **Short Data Retention Limits:** The law suggests data should be deleted once the "purpose is served" (often cited as 30–35 days). While good for privacy, this is a nightmare for **security forensics**. If a breach is discovered three months after it happened, the logs might have been legally deleted, making the investigation impossible.
 -
-

3. Ethical Concepts in Information Security

Ethics go beyond what is "legal" and focus on what is "right."

- **Liability & Accountability:** If a system is breached, who is at fault? The developer who left a bug, or the admin who didn't patch it? Accountability ensures every action in a system can be traced to a specific user.
 - **Privacy vs. Security:** This is the ultimate ethical dilemma. Does a company have the right to monitor employee emails (Security) at the cost of the employee's personal space (Privacy)?
 - **Responsible Disclosure:** If you find a bug in a bank's website, the ethical path is to tell the bank privately (White Hat) rather than selling it on the dark web (Black Hat).
-

4. Professional Standards and Organizations

Professionalism is defined by certifications and adherence to a strict **Code of Ethics**.

Major Professional Organizations

Organization	Focus Area
(ISC) ²	Known for the CISSP certification; emphasizes the "Common Body of Knowledge."
ISACA	Focuses on IT governance, risk, and auditing (CISA, CISM).
SANS Institute	Provides high-level technical training and maintains the GIAC certifications.

The (ISC)² Code of Ethics Canons

Security professionals (specifically CISSPs) must follow these four canons in strict order of priority:

1. **Protect society, the common good, and the infrastructure.** (Safety first!)
2. **Act honorably, honestly, justly, responsibly, and legally.**
3. **Provide diligent and competent service to principals.** (Do your job well for your employer.)
4. **Advance and protect the profession.** (Mentor others and maintain the field's reputation.)

3. Limitations in Professional & Ethical Practice

In Nepal, the "Professional" pillar of InfoSec also faces structural limitations:

- **Lack of Mandatory Standards:** In many countries, sectors like Banking *must* follow standards like ISO 27001. In Nepal, while the Central Bank (NRB) has guidelines, there is no broad national law forcing all critical infrastructure (hospitals, power grids) to follow specific security standards.
 - **The "Whistleblower" Risk:** Nepal lacks strong legal protection for "Ethical Hackers." If a security researcher finds a bug in a government system and reports it, they risk being arrested under the ETA 2063 for "unauthorized access," even if their intent was to help.
 -
-

Comparison of Law vs. Reality in Nepal

Feature	Legal Provision (The Theory)	Current Limitation (The Reality)
Cybercrime Court	Dedicated IT Tribunal.	Handled by Kathmandu District Court only.
Data Privacy	Consent is required for data use.	Most apps/sites in Nepal have vague terms.
Law Scope	Targets "Computer Crimes."	Frequently used to target "Online Speech."
Penalties	Up to 5 years jail / 1 Lakh	Fines are often too low for corporate

Feature	Legal Provision (The Theory)	Current Limitation (The Reality)
	fine.	breaches.

"Ethical Use Policy" that a Nepali IT company could use to stay compliant with the ETA 2063?

1. International Laws and Legal Bodies

Because cyberattacks often involve a hacker in Country A, a server in Country B, and a victim in Country C, international laws act as a common language for justice.

The Budapest Convention on Cybercrime

This is the only binding international instrument on this issue. It serves as a guideline for any country developing national cyber laws.

- **Substantive Law:** Defines crimes like illegal access, data interference, and child pornography.
- **Procedural Law:** Sets rules for how authorities can search computer networks and intercept data.
- **International Cooperation:** Mandates that member states help each other in cybercrime investigations.

Key International Bodies

- **INTERPOL/Europol:** These organizations have dedicated Cybercrime Centres that facilitate cross-border police cooperation.
- **UNODC (United Nations Office on Drugs and Crime):** Provides technical assistance to developing nations to help them draft cybercrime legislation.

2. Information Security Laws in Nepal

Nepal's legal landscape is currently in a state of transition. While the laws are being modernized, there are significant "grey areas."

A. Electronic Transactions Act (ETA), 2063 (2006)

Initially intended to facilitate e-commerce, this act has become the "Swiss Army Knife" for prosecuting cybercrime in Nepal.

Section	Offense	Penalty / Provision
Section 44	Piracy or Altering Source Code	Up to 3 years jail or NPR 2,00,000 fine.
Section 45	Unauthorized Access (Hacking)	Up to 3 years jail or NPR 2,00,000 fine.
Section 46	Damage to Computer System	Fine up to NPR 2,00,000 or jail up to 3 years .
Section 47	Publication of Illegal Materials	Prohibits "indecent" or "hate speech" online. Most controversial section.
Section 48	Confidentiality Breach	Punishes those who leak confidential digital data.

B. Individual Privacy Act, 2075 (2018)

This law was a milestone in protecting citizen data.

- **Consent First:** No organization (bank, hospital, or IT company) can collect your data without your explicit consent.
- **Sensitive Data:** Information regarding your caste, religion, biometrics, and health is strictly protected.
- **Right to be Forgotten:** Individuals can request that their data be deleted once the purpose of collection is served.

C. Limitations in Nepal

1. **Vague Language:** Terms like "indecent material" in Section 47 are subjective, leading to potential misuse against journalists or activists.

2. **Lack of Expertise:** While the law exists, there is a shortage of "Cyber Forensics" experts within the police force to gather evidence that stands up in court.
 3. **Cross-border Challenges:** Nepal lacks extradition treaties specifically for cybercriminals, making it hard to catch hackers attacking from abroad.
-

3. Ethical Concepts & Professionalism

In security, "can" does not mean "should." Professionals operate under a higher standard than the general public.

Ethical Concepts

- **Liability:** If you are a Lead Security Engineer and you fail to apply a critical patch, you might be held personally or civilly liable for the resulting breach.
- **The Golden Rule:** Treat others' data as you would want your own data treated.
- **Conflict of Interest:** A security consultant shouldn't recommend a firewall simply because they get a commission from the vendor.

Codes of Ethics (The "Vows" of a Professional)

Most certified professionals (like those with **CISSP** or **CISM**) must adhere to a code. For example, the **(ISC)² Code of Ethics** prioritizes the "Common Good" over the "Employer's Interests."

Why Join Professional Organizations?

Organizations like **ISACA** or the **Computer Association of Nepal (CAN Federation)** provide:

1. **Networking:** Access to a community of experts.
2. **Standards:** Guidelines on how to perform audits or risk assessments.
3. **Advocacy:** They lobby the government to improve the laws we discussed above.

"Do's and Don'ts" for a cybersecurity professional in Nepal to ensure they stay on the right side of both the ETA 2063 and the Privacy Act 2075?

1. Compliance with the Electronic Transactions Act (ETA) 2063

This law treats technical actions as legal events. Every bit you change could have legal consequences.

✓ DO:

- **Obtain Explicit Authorization:** Always get a written "Letter of Engagement" or a signed contract before performing any vulnerability assessment or penetration testing. Under **Section 45**, "unauthorized access" is a crime, regardless of your intent.
- **Use Licensed Software:** Ensure all servers and organizational tools are licensed. **Section 44** protects source code and intellectual property; using cracked tools can make you liable.
- **Keep Audit Logs:** Maintain detailed logs of all administrative actions. In the event of a breach, these logs are your primary evidence to prove that you acted with "due diligence."
- **Secure Digital Signatures:** Treat digital signatures as physical stamps. Under the ETA, a digital signature is legally binding for contracts and official government filings.

✗ DON'T:

- **Perform "Drive-by" Hacking:** Even if you find a bug in a Nepali website (like a bank or government portal), do not attempt to "test" it without permission. You could be prosecuted under **Section 46** for "damage to computer systems."
 - **Share "Indecent" or "Hate Speech":** **Section 47** is extremely broad. Avoid hosting, sharing, or failing to moderate content that could be interpreted as jeopardizing social harmony or public morality.
-

2. Compliance with the Individual Privacy Act 2075

This act focuses on the "Right to be Let Alone." For a security professional, this means handling user data with extreme care.

✓ DO:

- **Implement "Purpose Limitation":** Only collect data that is strictly necessary for your service. If you collect a user's phone number for 2FA, you cannot legally use it for marketing without a separate consent.
- **Practice "Data Minimization":** Delete data once its purpose is served. The law mandates that personal information must be destroyed within **30 days** of achieving the purpose of collection (unless other laws require longer retention).
- **Appoint a Privacy Officer:** If you are at a senior level, ensure your organization has a designated person responsible for data privacy compliance.

✗ DON'T:

- **Process "Sensitive Information" Without Consent:** Information about a person's caste, religion, health, or biometrics is "Sensitive." Processing this without a very specific legal basis or explicit written consent can lead to fines up to **NPR 5,00,000**.

- **Export Data Illegally:** Be cautious with cloud storage. The **IT Bill** (currently in progress) and privacy guidelines suggest that sensitive data of Nepali citizens should preferably stay within the country's borders.
-

Summary Comparison for Professionals

Aspect	The "Law-Abiding" Path	The "Risky" Path
Testing	Authorized Pen-Testing with a contract.	Unauthorized "Bug Hunting" for fun.
Data Storage	Encrypted, consented, and temporary.	Plain-text, unconsented, and permanent.
Communication	Professional, filtered, and respectful.	Spreading unverified or "indecent" info.
Software	Commercial Licensed or verified Open Source.	Pirated software and "cracks."

Professional Ethical Guidelines

Beyond the laws, follow the **(ISC)² Canons** adapted for the Nepali context:

1. **Protect the State and its People:** Ensure your work doesn't accidentally disrupt critical national infrastructure (like Nepal Electricity Authority or Nepal Telecom systems).
2. **Act Honestly:** Never overstate a security risk to scare a client into buying more services.
3. **Competence:** If a task (like advanced Forensics) is beyond your skill level, refer it to a specialist.

how the new "IT Bill" (currently in parliament) intends to address these limitations, and why it is also facing heavy criticism?

To address the gaps in the aging **Electronic Transactions Act (ETA) 2063**, the Nepal government introduced the **Information Technology and Cybersecurity Bill (2082/2025-26)**.

1. How the IT Bill Addresses Past Limitations

The new bill attempts to provide a more comprehensive framework than the ETA 2063 by adding several modern provisions:

- **Mandatory Licensing for Data Centers:** Unlike the old law, the new bill requires all Data Centers and Cloud Service providers operating in Nepal to obtain a formal license. This aims to standardize security protocols across the country.
 - **Registration of Social Media Platforms:** Global giants like Facebook, X (Twitter), and TikTok are required to register in Nepal and appoint a local "Point of Contact." This is intended to solve the "Offshore Entity Loophole" by making these companies legally accountable to Nepali authorities.
 - **Recognition of Emerging Tech:** It introduces preliminary language for regulating **AI (Artificial Intelligence)**, IoT, and Blockchain, which were entirely absent from the 2006 law.
 - **Heftier Penalties:** Financial penalties have been significantly increased. For example, operating an unlicensed social media platform can lead to fines up to **NPR 2.5 million**.
-

2. Critical Limitations and "The Controversy"

Despite these updates, legal experts, journalists, and human rights activists have raised serious red flags regarding the bill's current draft:

A. Threat to Freedom of Expression (The New "Section 47")

Critics argue that the bill simply "repackages" the problematic Section 47 of the old ETA.

- **Vague Terminology:** The bill prohibits content that undermines "national unity," "sovereignty," or is "obscene." Since these terms are not strictly defined, there is a risk they could be used to silence political dissent or satire.
- **Harsh Sentencing:** Posting "offensive" comments can carry higher penalties (up to 5 years in jail) than some physical crimes, which critics call a "disproportionate" use of the law.

B. Increased Surveillance and Privacy Risks

- **Mandatory Identity Verification:** The bill suggests that social media users should not be anonymous. This removes the "right to anonymity," which is often crucial for whistleblowers and activists.
- **Direct Content Removal:** Authorities can direct platforms to remove content immediately. If a platform refuses, the government has the power to block the entire service in Nepal (similar to the temporary TikTok ban of 2023).

C. Data Privacy Gaps

- **Limited Data Rights:** While the bill mentions data protection, it lacks the "Rights of the Data Subject" found in international laws like GDPR (e.g., the right to correct data or the right to data portability).
 - **35-Day Deletion Rule:** The requirement to destroy personal data within 35 days of its purpose ending remains a major limitation for **Cyber Forensics**. Professionals argue that most breaches are only discovered months later, by which time the evidence would have been legally deleted.
-

3. Comparison: ETA 2063 vs. The New IT Bill (2082)

Feature	ETA 2063 (Current)	IT Bill 2082 (Proposed)
Main Focus	E-Commerce & Digital Signatures	Cybersecurity & Social Media Regulation
Social Media	Not mentioned	Mandatory Registration & Local Office
Data Privacy	Very basic	Specific provisions, but lacks user rights
Cloud/Data Centers	Unregulated	Mandatory Licensing required
Cybercrime Court	Tribunal (Mostly non-functional)	IT Tribunal (Proposed to be more active)

Summary of the "Limitation" Context

The primary limitation is no longer a "lack of law," but rather the "**over-reach of law.**" For a cybersecurity professional, this means:

1. **Compliance is harder:** You now have to worry about platform registration and specific data center licenses.
2. **Liability is higher:** The fines are much larger.

3. **Ethical Conflict:** You may be asked by authorities to provide data or remove content under vague "national security" claims, creating a conflict with professional ethics regarding user privacy.