



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Cybersecurity: A Legal Perspective

Objectives

- To understand the legal aspects of cybersecurity
- To understand the importance of legislation in cybersecurity

Introduction

Having looked at case studies of hackers misusing the internet and the cyberspace to perpetrate malicious attacks, what does the law say about cybercrime? Due to the increasing cost and damage of cybercrime, there is dire need for countries to pass laws designed to prevent cyber-attacks and prosecute cyber criminals. Cybersecurity laws and regulations act as directives to aid institutions in the implementation of cybersecurity safeguards to protect them from cyber-attacks. These laws also establish offenses and their respective penalties. The heavy fines and penalties are used to deter cyber attackers from committing cybercrime. It is crucial to have an understanding of these laws as they put into perspective the extent of the damage caused by cyber-attacks and the government's cybersecurity efforts to curb cybercrime and thwart cyberterrorists.

Common provisions and directives in cybersecurity laws include:

- Increasing penalties for computer crime or addressing specific crimes, e.g., ransomware, unauthorized access, phishing etc.
- Requiring government agencies to implement training or specific types of security policies
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.
- Supporting programs or incentives for cybersecurity training and education.

In this article, you will explore various cybersecurity laws and legal stipulations. Globally, 154 countries (79%) have enacted cyber laws. To check whether your country has implemented any cybersecurity laws, you can utilize the United Nations Conference on Trade and Development (UNCTAD) [website](#).

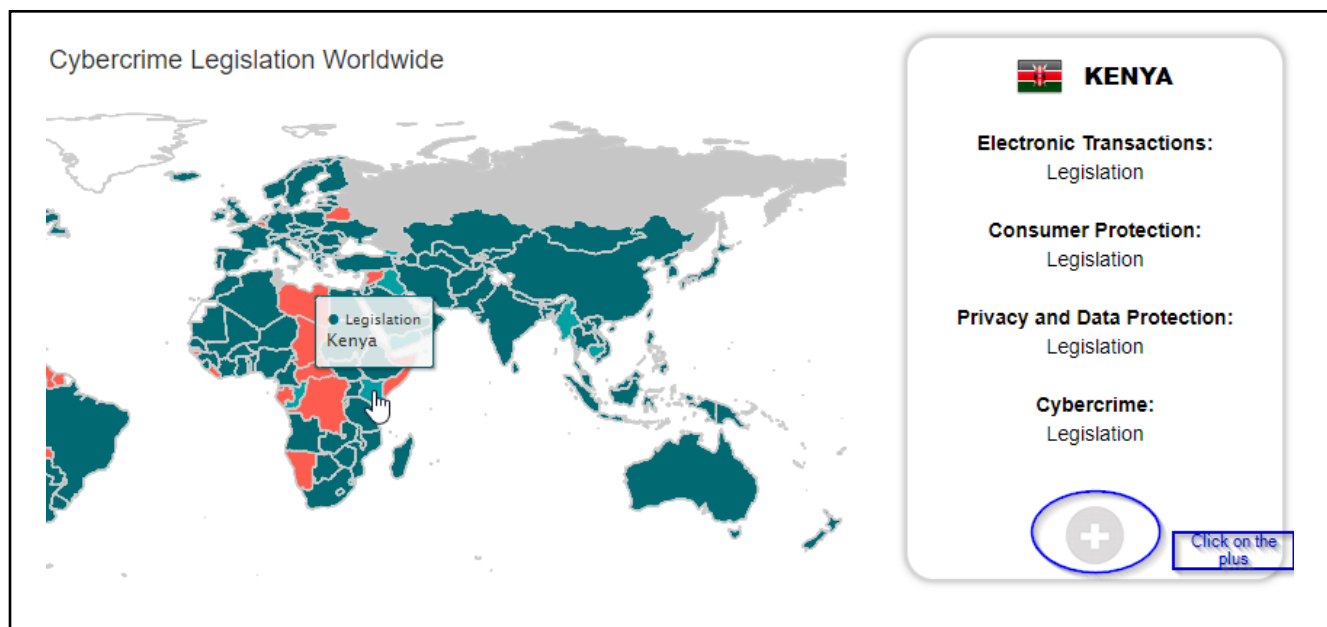
Steps to follow:

1. Click on the link above.
2. On the map provided on the site, click on your country.
3. Click on the Plus (+) to expand and read more on the laws. This will show various legislations grouped in categories such as data protection, cyber laws and consumer protection laws.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Below is an example of checking Kenya's cybersecurity laws using the steps above.



Cyber security legislation from UNCTAD

Cyberlaw Tracker: The case of Kenya

Region: African Union

Community of Sahel-Saharan States

Common Market for Eastern & Southern Africa

East African Community

Intergovernmental Authority on Development

Consumer Protection Laws	Cybercrime Laws	
	Legislation	Kenya Information and Communication Act, 1998 (in English) The computer misuse and cybercrimes Act, 2018
Cybercrime Laws		
Data Protection & Privacy Laws		
E-Transactions Laws		

Cyber security legislation from UNCTAD



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Kenya: Computer Misuse and Cybercrimes Act 2018

The Computer Misuse and Cybercrimes Act was enacted in 2018 to protect the confidentiality, integrity and availability of computer systems, programs and data. The Act also provides guidelines for investigation, prosecution and punishment of cybercrimes.

Some of the key provisions in the Act include:

- The Act establishes various computer misuse and cybercrime offences including unauthorized interference or interception of computer systems programs or data, false publication of data, cyber harassment, cyber terrorism, identity theft and impersonation, phishing, computer fraud, computer forgery, unauthorized disclosure of passcodes, fraudulent use of electronic data among others.
- The Act prescribes hefty penalties for contravention of its provisions. These include fines as significant as 50,000 US dollars, imprisonment of up to 20 years, confiscation of assets purchased from proceeds of an offence and compensation.
- The Act requires service providers to assist in investigation of offences e.g. by collecting and providing data to the investigation officers.
- The Act also establishes investigation procedures for search and seizure, real-time collection of data and evidence preservation.

European Union: General Data Protection Regulation (GDPR)

The GDPR is a set of rules and legal provisions imposed on the European Union member states. The main aim of the GDPR is to ensure that EU citizens have more control over their data. It applies to all organizations that collect and process EU citizens' data.

The GDPR is very similar to the UK's Data Protection Act of 1998.

Some of the key provisions in the GDPR include:

- Consent: Any organization handling sensitive data must seek consent every time they access the data. Consent agreements should be concise and clear.
- Right to access: Owners of any data have the right to request confirmation on what data is being processed and for what purpose.
- Breach notification: Companies to notify all data subjects that a security breach has occurred within 72 hours of first discovering it.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- Right to be forgotten: Companies are required to erase all personal data when asked to do so by the owner of the data (data subject).



Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA contains a number of provisions applicable to data protection and cybersecurity, including:

- Organizations are responsible for personal information under their control and must designate an individual or individuals who are accountable for compliance with the principles set out in Schedule 1 of PIPEDA.
- Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
- Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, format of the information, and the method of storage.
- The methods of protection should include (a) physical measures – e.g., locked filing cabinets and restricted access to offices; (b) organizational measures – e.g. security clearances and limiting access on a "need-to know" basis; and (c) technological measures – e.g. the use of passwords.

Canada has quite a number of laws and frameworks governing cybersecurity and data protection. Most of these laws are based on principles established in the to erase Canadian Standards Association Model Code for the Protection of Personal Information⁷ (CSA Model Code).

These 10 principles include:

- accountability,
- identifying purposes,
- consent,
- limiting collection,
- limiting use, disclosure and retention,
- accuracy,
- safeguards,
- openness,
- individual access and
- challenging compliance.

India: Information Technology Act, 2000

The Act contains some of the most stringent privacy requirements in the world. The Act creates punishable offenses for the following:

- Tampering with computer source documents.
- Publishing or transmitting obscene material in electronic form.
- Publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form.
- Breach of confidentiality and privacy.
- Punishment for disclosure of information in breach of lawful contract.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- Penalty for publishing electronic signature Certificate false in certain particulars.
- Publication for fraudulent purposes, among others.

India also has an ICT policy for school education. The initiative of ICT Policy in School Education is inspired by the tremendous potential of ICT for enhancing outreach and improving quality of education. This policy endeavors to provide guidelines to assist the States in optimizing the use of ICT in school education within a national policy framework.

It is important to know and understand the cyber security and data protection laws that exist in your country. This will guide you on how to report cybercrime as well as govern your interaction with digital technology lest you commit an offence unknowingly. Remember, ignorance is not a defense.