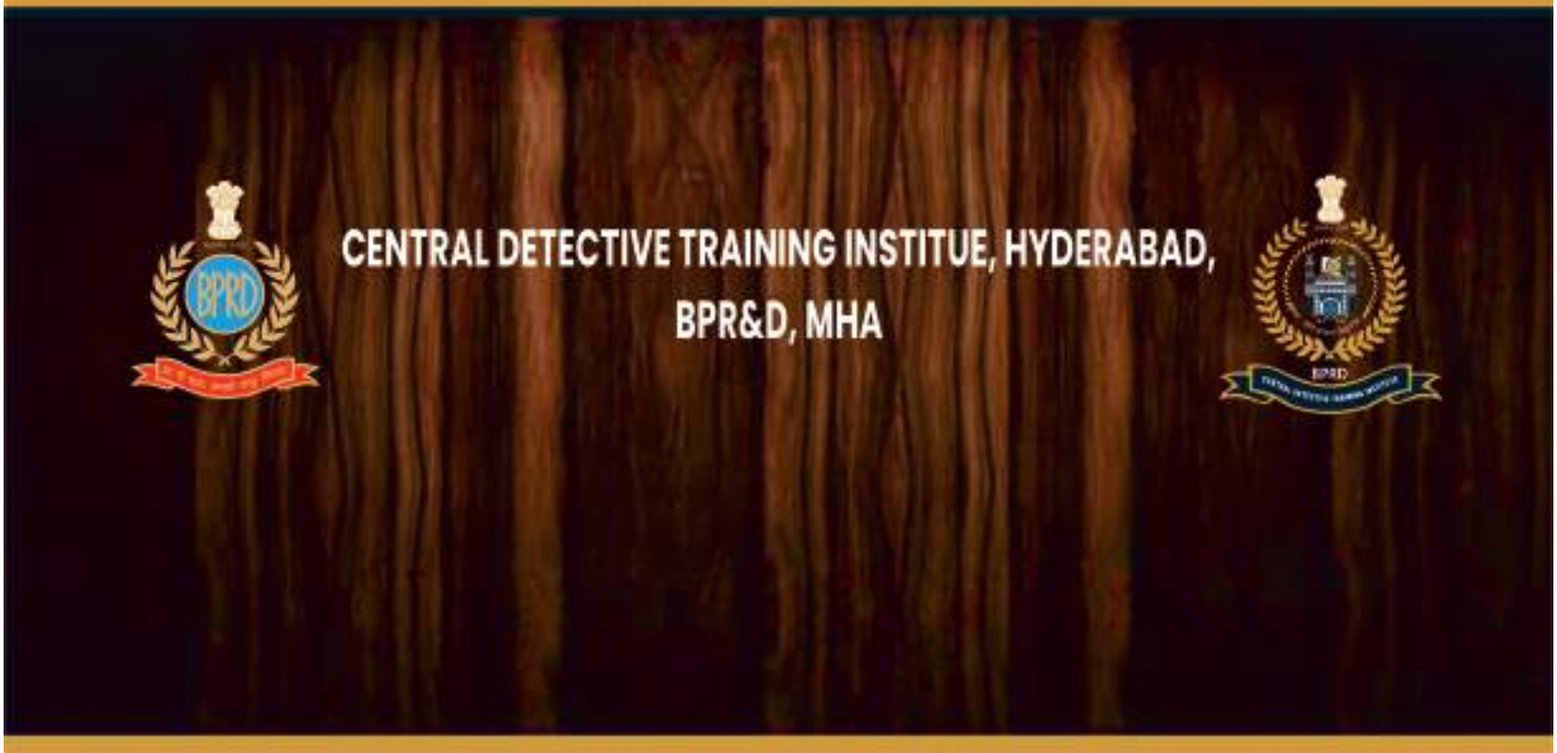
October - December, 2025

CDTI, HYDERABAD *Bulletin*

HORIZON

Our Motto "ज्ञानं सम्यग् वेक्षणम्" which means
"WISDOM LIES IN PROPER PERSPECTIVE"



A Quarterly Bulletin of Central Detective Training Institute, Hyderabad

MESSAGE OF THE DIRECTOR

Salmantaj Patil, IPS
DIRECTOR

It gives me immense pleasure that the Central Detective Training Institute, Hyderabad is going to launch its quarterly year news magazine **"HORIZON"** for the period October to December, 2025.

CDTI, Hyderabad designated to be the Centre of Excellence for **"Police Technology, IT and Cybercrime".** With the establishment of **"National Cyber Research, Innovation and Capacity Building Centre (NCRI&CB)"** under the Indian Cyber Crime Coordination Centre (I4C), MHA in CDTI-Hyderabad the Institute is striving for capacity building in the Law Enforcement Agencies. In order to find solutions to pressing issues of LEAs, CDTI-Hyderabad successfully conducted a National Police Hackathon in collaboration with Telangana Cyber Security Bureau & Indian School of Business, Hyderabad. The proposals received were sent to the Modernization Division of BPR&D for further action.

CDTI is also interacting with its client states for identifying the training and coordinating on issues faced by the States. Feedback related to New Criminal Laws courses from the ground level is obtained by visiting the police stations in different states which is submitted to the Ministry of Home Affairs, Govt of India.

CDTI is striving hard to be a Centre of Excellence in the topic of 'Police Technology, IT & Cyber Crime'.

CONTENTS

Front view of Admin building of CDTI, Hyderabad

COURSES CONDUCTED FROM OCT TO DEC, 2025

From 01st Oct to 31st Dec, 2025 a total of 22 Courses (including Workshops, Webinars, Conferences) were conducted in which 735 Officers were trained.

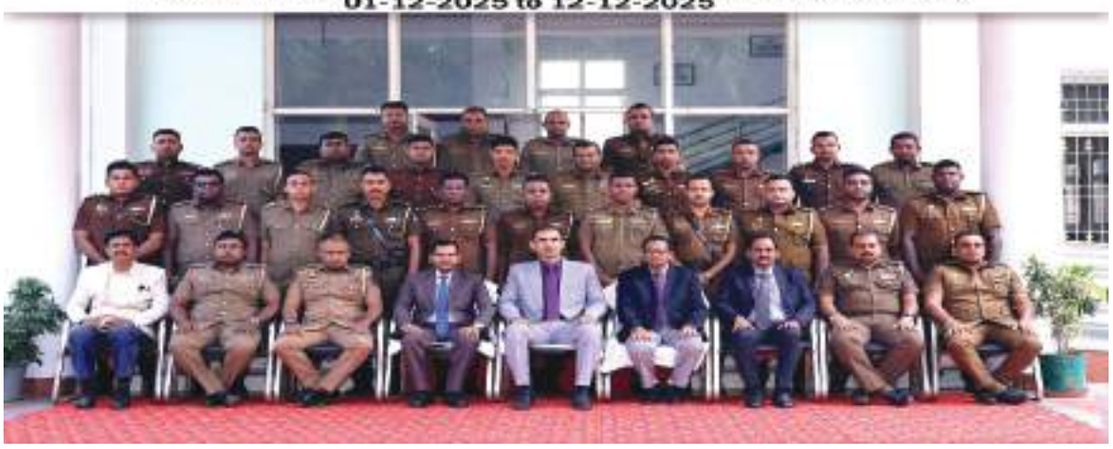
S. No	Name of the Course	Date		No. of Participants
		From	To	
1	Workshop on Drone-based geolocation and mapping in crime investigation & Anti-Drone Technology	03.10.2025	03.10.2025	55
2	Part 3 TOT NCL for Batch 3 & 4 (in collaboration with PMA Team)	06.10.2025	10.10.2025	36
3	Preserving Digital Evidence: Chain of Custody and Best Practices	06.10.2025	10.10.2025	31
4	Interrogation techniques and the surrender of Maoists/ Militants	13.10.2025	17.10.2025	20
5	Data-Driven Predictive Policing, AI-Based Crime Analysis, Intelligence Gathering, and Data Analytics in Law Enforcement	13.10.2025	17.10.2025	24
6	Webinar on Investigating Cybercrime using Artificial Intelligence & A-I based crime analysis	24.10.2025	24.10.2025	54
7	Protection of data and digital public goods	27.10.2025	31.10.2025	20
8	Workshop on investigating cybercrime in the context of 5G networks	07.11.2025	07.11.2025	81
9	Investigation of Cyber Crime against Women, Children and their safety related issues	10.11.2025	14.11.2025	29
10	Investigation of Cyber Crime against Women, Children and their safety related issues (**Exclusively for 05 Royal Bhutan Police Officers)**	10.11.2025	14.11.2025	5
11	Basic course on Cyber Crime Investigation and Digital Forensics	10.11.2025	14.11.2025	22
12	Intermediate course on Cyber Crime Investigation and Digital Forensics	17.11.2025	21.11.2025	22
13	Investigation of Dark Web, Deep web & Crypto Currency	17.11.2025	21.11.2025	24
14	Advanced Scientific Investigation Course (**Exclusively for Royal Bhutan Police Officers)**	24.11.2025	05.12.2025	20
15	Collection and Preservation of Digital Evidence (DSI), Chain of custody, BSA, IT Act – Technological aspects under NCL	24.11.2025	28.11.2025	22

S. No	Name of the Course	Date		No. of Participants
		From	To	
16	Counter Radicalization, Human Intelligence, Effective Policing, and SC Judgment on Maoist/Militant Surrender	24.11.2025	28.11.2025	20
17	ITEC course on Handling Crime Investigation **(For Sri Lankan Police Officers)**	01.12.2025	12.12.2025	29
18	Cyber Terrorism, State-Sponsored Attacks, Espionage, and National Defence: Securing Military and Government Networks	01.12.2025	05.12.2025	20
19	Webinar on Cyber terrorism and National Security: Understanding the Evolving Threat Landscape, Gathering of intelligence; Use of global Technology & software	23.12.2025	23.12.2025	75
20	Online Conference on "Cloud Forensics: Uncovering evidence in the Cloud infrastructure	24.12.2025	24.12.2025	25
21	Seminar on implementation of NCL and practical difficulties faced by police (Exclusively Telangana Police)	29.12.2025	29.12.2025	76
22	Crypto currencies and cybercrime: Tracking the Financing of Terror & Misuse of Crypto-Currency	29.12.2025	02.01.2026	25
TOTAL				**735**

ITEC (Indian Technical and Economic Cooperation) courses

- Conducted two weeks course on **'Handling Crime Investigation'** at CDTI, Hyderabad from 01.12.2025 to 12.12.2025 for **Sri Lankan Police Officers in which 29 officers have participated**

Inauguration Ceremony of ITEC Course on "Handling Crime Investigation" on 01.12.2025. Dr. N Venkanna, Joint Director, CLUES Team, Hyderabad Police was graced the event as the Chief Guest being presented planter by the Director, CDTI, Hyderabad



Valedictory Ceremony of ITEC Course on "Handling Crime Investigation" on 12.12.2025. Dr. S K Mohanka, DIG/ CASO, CISF, Airport Unit, Hyderabad graced the Valedictory programme as Chief Guest being presented planter by the Director, CDTI, Hyderabad.

Course for Royal Bhutan Police Officers

I. Conducted two weeks course on **Advanced Scientific Investigation'** at CDTI, Hyderabad from 24.11.2025 to 05.12.2025 for **Royal Bhutan Police** Officers in which 20 officers have participated

Inauguration Ceremony of Course on "Advance Scientific Investigation" on 24.11.2025. Dr. P V Ramasastry, IPS, DGP (Retd), Uttar Pradesh was graced the event as the Chief Guest being presented Memento by the Director, CDTI, Hyderabad

II. Conducted one week course on **'Investigation of Cyber Crime against Women, Children and Their Safety related issues'** at CDTI, Hyderabad from 10.11.2025 to 14.11.2025 for **Royal Bhutan Police Officers in which 05 officers have participated**

Seminar on NCL

- CDTI, Hyderabad is conducted a Seminar on **"Implementation of New Criminal Laws (NCL) and practical difficulties experienced by the Telangana Police"** on 29.12.2025. Police officers from all Commissionerate's of Telangana State, Prisons Department and Public Prosecutors from Department of Prosecution of Telangana and their teams who are well versed with the subject were attended the Seminar. No. of participants is 76.

Inauguration Ceremony of Seminar on "Implementation of New Criminal Laws (NCL) and practical difficulties experienced by the Telangana Police" on 29.12.2025. Ms. Charu Sinha, IPS, ADGP(CID), TG inaugurated the Seminar as Chief Guest. Sh S. Sambasiva Reddy DoP; Sh.Narayan Naik, IPS, DIG CID & Sh. Salmantaj Patil, IPS, Director, CDTI Hyderabad were present on the occasion

Group Photo of Seminar on "Implementation of New Criminal Laws (NCL) and practical difficulties experienced by the Telangana Police"

AWARENESS PROGRAMMES

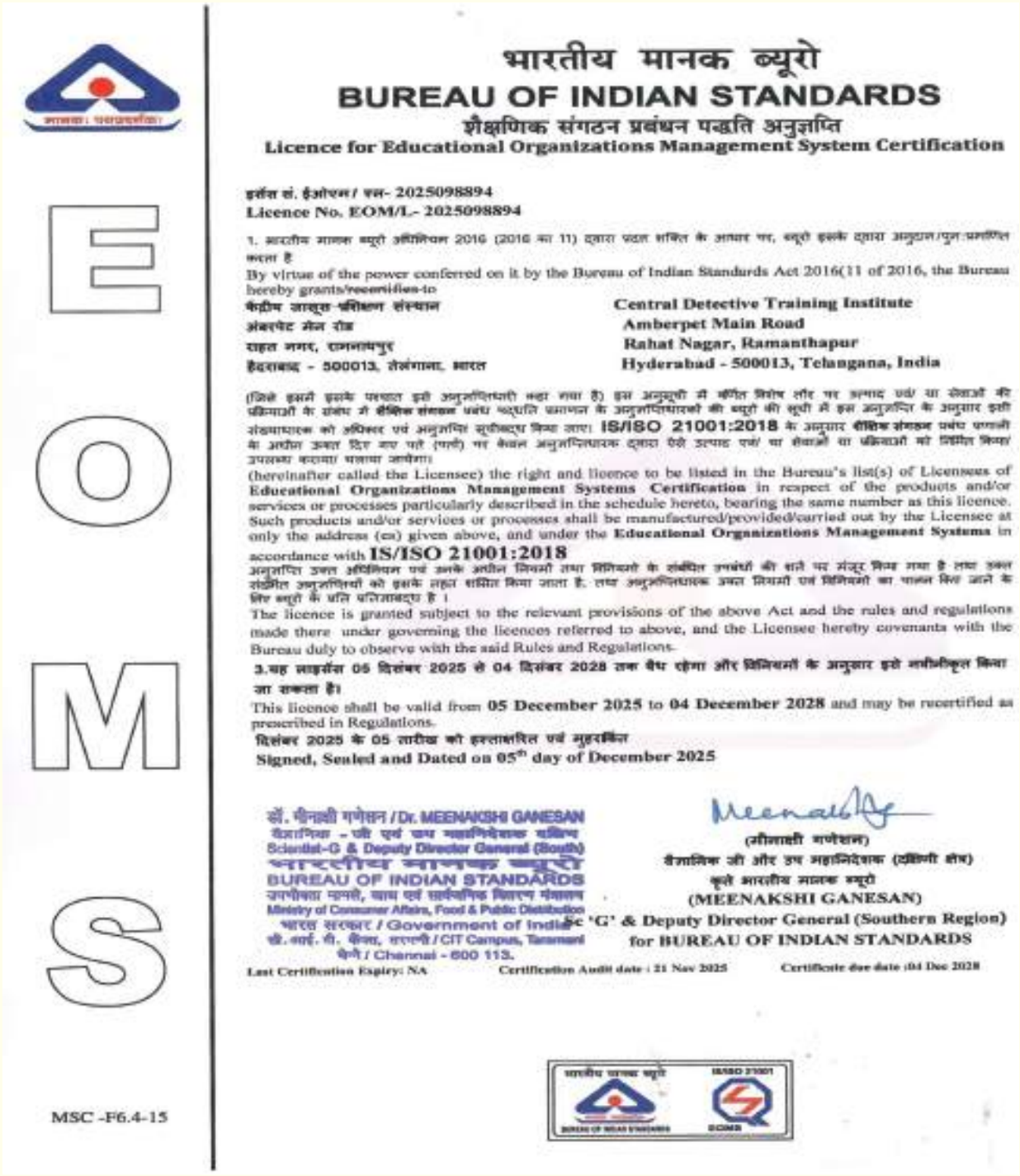
- Conducted Cyber Awareness Programme on **"Measure of Social media Cyber & Social Media Crimes-Ways to prevent them"** on 22-12-2025 for students of ZPHS, Ramanthapur, Hyderabad. 44 students and 3 teaching faculty are participated in the programme.

- Conducted Cyber Awareness Programme on **"ATM & Digital Payment Frauds"** on 06-11-2025 for students of Megha Junior College, Ramanthapur, Hyderabad. 30 students and 2 faculty members participated in the programme.

- Conducted Awareness Programme on **Cyber Awareness & Safety of Women** on 23.10.2025 for the students of Mega Junior College, Hyderabad. 107 students/teaching staff have participated. After the programme, students visited Classrooms and NCRI&CB lab of CDTI, Hyderabad.

BIS Accreditation

- CDTI, Hyderabad has got **Certification of Educational Organizations Management Systems IS/ISO 21001:2018 with Licence No. EOM/L – 2025098894 by Bureau of Indian Standards (BIS)** which is valid from 05.12.2025 to 04.12.2028.



भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
शैक्षणिक संगठन प्रबंधन पद्धति अनुज्ञप्ति
Licence for Educational Organizations Management System Certification

E O M S

लाइसेंस सं. ईओएम/ एल- 2025098894
Licence No. EOM/L- 2025098894

1. भारतीय मानक ब्यूरो अधिनियम 2016 (2016 का 11) द्वारा प्रदत्त शक्ति के आधार पर, ब्यूरो इसके द्वारा अनुज्ञप्ति/पुन:प्रमाणित करता है
By virtue of the power conferred on it by the Bureau of Indian Standards Act 2016(11 of 2016, the Bureau hereby grants/recertifies to

केंद्रीय जासूस प्रशिक्षण संस्थान
अंबरपेट मेन रोड
राहत नगर, रामनाथपुर
हैदराबाद - 500013, तेलंगाना, भारत

Central Detective Training Institute
Amberpet Main Road
Rahat Nagar, Ramanthapur
Hyderabad - 500013, Telangana, India

(जिसे इसमें इसके पश्चात इसी अनुज्ञप्तिधारी कहा गया है) इस अनुसूची में वर्णित विशेष तौर पर उत्पाद एवं/ या सेवाओं और प्रक्रियाओं के संबंध में शैक्षिक संगठन प्रबंध पद्धति प्रमाणन के अनुज्ञप्तिधारकों की ब्यूरो की सूची में इस अनुज्ञप्ति के अनुसार इसी संख्यात्मक को अभिकर्ष एवं अनुज्ञप्ति सूचीबद्ध किया जाए। IS/ISO 21001:2018 के अनुसार शैक्षिक संगठन प्रबंध पद्धतियों के अधीन उक्त दिए गए पते (पतों) पर केवल अनुज्ञप्तिधारक द्वारा ऐसे उत्पाद एवं/ या सेवाओं या प्रक्रियाओं को विनिर्मित किया/ उपलब्ध कराया/ चलाया जायेगा।
(hereinafter called the Licensee) the right and licence to be listed in the Bureau's list(s) of Licensees of **Educational Organizations Management Systems Certification** in respect of the products and/or services or processes particularly described in the schedule hereto, bearing the same number as this licence. Such products and/or services or processes shall be manufactured/provided/carried out by the Licensee at only the address (es) given above, and under the **Educational Organizations Management Systems** in accordance with **IS/ISO 21001:2018**

अनुज्ञप्ति उक्त अधिनियम एवं उसके अधीन नियमों तथा विनियमों के संबंधित उपबंधों की शर्तों पर मंजूर किया गया है तथा उक्त संलग्नित अनुज्ञप्तिधारी को इसके तहत शामिल किया जाता है, तथा अनुज्ञप्तिधारक उक्त नियमों एवं विनियमों का पालन किए जाने के लिए ब्यूरो के प्रति प्रतिज्ञाबद्ध है ।
The licence is granted subject to the relevant provisions of the above Act and the rules and regulations made there under governing the licences referred to above, and the Licensee hereby covenants with the Bureau duly to observe with the said Rules and Regulations.

3.यह लाइसेंस 05 दिसंबर 2025 से 04 दिसंबर 2028 तक वैध रहेगा और विनियमों के अनुसार इसे नवीनीकृत किया जा सकता है।
This licence shall be valid from **05 December 2025** to **04 December 2028** and may be recertified as prescribed in Regulations.

दिसंबर 2025 के 05 तारीख को हस्ताक्षरित एवं मुहरबंद
Signed, Sealed and Dated on 05th day of December 2025

डॉ. मीनाक्षी गणेसन / Dr. MEENAKSHI GANESAN
वैज्ञानिक - जी एवं उप महानिदेशक दक्षिण
Scientist-G & Deputy Director General (South)
भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
उपभोक्ता मामले, खाद्य एवं सार्वजनिक वितरण मंत्रालय
Ministry of Consumer Affairs, Food & Public Distribution
भारत सरकार / Government of India
सी. आई. टी. कैम्पस, तरामणी / CIT Campus, Taramani
चेन्नै / Chennai - 600 113.

Meenakshi

(मीनाक्षी गणेसन)
वैज्ञानिक जी और उप महानिदेशक (दक्षिणी क्षेत्र)
कृते भारतीय मानक ब्यूरो
(MEENAKSHI GANESAN)
Sc 'G' & Deputy Director General (Southern Region)
for BUREAU OF INDIAN STANDARDS

Last Certification Expiry: NA | Certification Audit date : 21 Nov 2025 | Certificate due date :04 Dec 2028

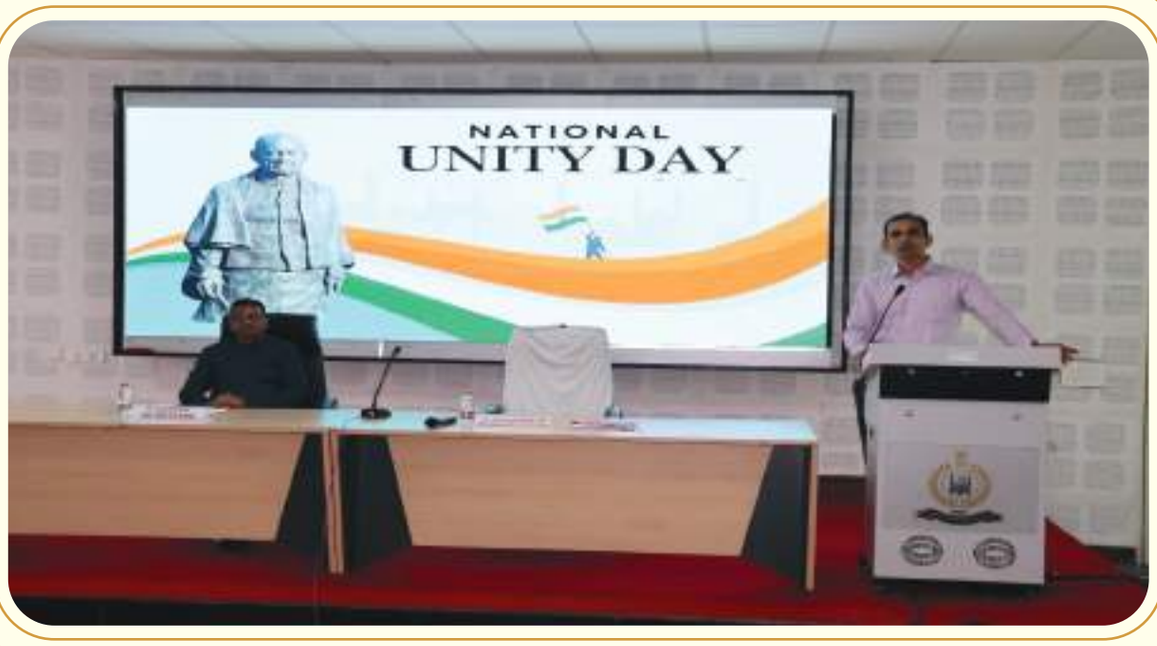
MSC -F6.4-15

61st Foundation Day of CDTI, Hyderabad

- Celebrated 61st Foundation Day of CDTI, Hyderabad at the Seminar Hall of CDTI, Hyderabad on 06.10.2025. Smt. Abhilasha Bisht, IPS, Director, RBVRR Telangana Police Academy graced the event as Chief Guest and Dr. Rajiv Giroti, Director, CFSL, Hyderabad graced the event as Special Guest.

Rashtriya Ekta Diwas

The National Unity Day 2025 of India (Rashtriya Ekta Diwas) observed on 31st October at CDTI, Hyderabad by taking pledge with the Staff and trainees which honors the 150th birth anniversary of the Iron Man of India, Sardar Vallabhbhai Patel.



GUIDELINES FOR AVOIDING CYBERCRIME VICTIMISATION

Sh.CH Malhal Rao,
SP (Retd.),
TG Police, Hyderabad

In today's digital world, cybercrime has become a major problem. Using technology, fraudsters are stealing people's personal and financial information, causing significant harm. Cybercriminals are luring innocent people into traps through various fraudulent methods.

Cybercrimes have become increasingly prevalent as individuals and businesses increasingly rely on digital platforms for their daily activities.

The amount of money people are losing to cybercrime is in the thousands of crores of rupees. According to 2024 statistics, India suffered losses exceeding ₹ 11,300 crore in the first nine months alone due to cybercrime.

Experts estimate that this loss could reach ₹ 20,000 crore by 2025. To avoid falling victim to these scams, it is crucial to increase awareness about cybersecurity.

A **victim of cybercrime** should act **immediately**, especially during the **"golden hour"** (the first few hours after the incident), as quick action can prevent financial loss and help trace the offender.

The victim should **disconnect the affected device from the internet**, **not delete any evidence** (messages, emails, transaction IDs, screenshots), and **inform the bank or digital wallet provider at once** to block cards, accounts, or UPI access. In cases of online financial fraud, the victim must **call the national cybercrime helpline number 1930 immediately**, which operates 24×7 in India.

The victim should also **register a complaint on the National Cyber Crime Reporting Portal (www.cybercrime.gov.in)** as soon as possible, preferably within the golden hour, to improve chances of fund recovery.

Changing passwords, enabling two-factor authentication, and alerting contacts about possible misuse of accounts are essential. Prompt reporting, awareness, and preservation of digital evidence play a crucial role in protecting the victim and enabling law enforcement to take swift action.

SOME OF THE COMMONLY REPORTED CYBERCRIMES INCLUDE:

1. Fake Customer Care Fraud:

Fraudster registers his number as customer care for e-commerce, e-wallets, couriers, and other sites. When an individual searches for customer care on any site, a fraudster's post pops up, and individuals contact fraudsters and end up in the trap of fraudsters.

Precautions:

- Contact the customer care number within the application or sites.
- Do not search for customer care numbers on Google or any other search engine.

2. KYC Update Fraud

Fraudsters send a message stating that your PAYTM/SBI/any other KYC is not current and ask you to contact a number. After contacting the number, the fraudsters collect card details by asking you to download remote access apps or fill in Google View forms, thereby cheating the innocent. In some instances, fraudsters ask you to send a nominal amount, such as Rs. 1 or 5, to the account provided by them. While making this transaction, fraudsters capture the credentials and make fraudulent transactions.

Precautions:

- Never respond to phishing emails/messages asking to update Paytm/SIM/ Bank Account KYC.
- It is advised not to install any applications such as Team Viewer, Quick Support, AnyDesk, etc., that support remote control access.

3. Card Skimming Frauds

a) At ATM Centres: -

A skimmer is a device used to copy debit or credit card data that fraudsters utilise to duplicate cards and withdraw amounts. Skimmers are also installed in ATM centres to collect your card data.

Precautions:

- People are advised to use their debit/credit cards personally and not give them to anyone for any transaction.
- To keep card details like a PIN, CVV, OTP, etc, secret, do not share with any one
- Advised to use chip-based Credit/debit Cards
- Check the alert messages from banks periodically on your registered mobile number
- and report any issues if you do not receive notifications.

b) At Restaurants/bars:

Fraudsters hire stewards from bars and restaurants and ask them to skim the Debit/Credit card data and note down the PIN. They then create duplicate cards by copying the card data onto plastic cards with magnetic strip readers and withdrawing amounts from ATM centres, thereby cheating the cardholders.

Precautions:

- Do not disclose the PIN card number to anyone.
- Not to hand over the cards to the employees while making transactions.

4. Vishing Calls

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorised entities. A **vishing** attack can be conducted via voice email, VoIP (voice over IP), landline, or cellular telephone.

Precautions:

- Don't respond to calls/emails with information related to bank details.
- Bankers never ask for your card details, including Card Number, PIN, CVV, OTP, etc., over the phone or by mail.
- People are advised to use their debit/credit cards personally and not give them to anyone for any transaction.
- Keep the Aadhar cards, PAN and identity details confidential and do not share them with anybody.
- Check the alert messages from banks periodically on your registered mobile number and report any issues if you do not receive notifications.

5. Phishing Mails

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising itself as a trustworthy entity in an electronic communication. **Phishing emails** may contain links to websites that distribute malware.

Precautions:

- Don't respond to emails with information related to bank details.
- Don't click on suspicious links
- Don't open attachments received from unknown senders.
- Use strong Anti-Virus software to avoid virus/malware attacks.

6. Advertising Portal Fraud

Using OLX, Quikr, etc., as a platform, fraudsters post vehicles and mobiles for lower prices and claim to be defence employees. Innocents pay fees in advance, believing them to be genuine. Most fraudsters ask to scan a QR code they send.

Precautions:

- Please don't believe vehicles/mobile phones sell at low prices.
- Verify products/vehicles physically before purchasing from OLX or any other platform.
- Please do not believe any claim can be made by the Defence by posting their photos and IDs while selling/purchasing the products.

7. Job Frauds

Fraudsters collect the database of job seekers from Naukri.com, Shine.com, Indeed, and timesjobs.com, mail or call them offering jobs in MNCs, and collect fees for registration, security deposit, etc.

Precautions:

- Don't encourage backdoor entry to jobs.
- Verify the genuineness of the offer letter received through HR, Friends and employees working in the same company.
- Please don't believe emails offering jobs, which may be similar to genuine sites like Naukri, Indeed, LinkedIn, etc.
- Fraudsters use many spoofing applications in the name of MNCs to verify that candidates can call back that number.

8. Loan Frauds

Borrowers misuse the bank's trust by submitting fake documents. There are agents in the market who specialise in duplicating documents. With the emergence of new technologies, they (agents) have become experts in faking documents, and their number is increasing.

Precautions:

- Don't trust loan offers below the bank rate of interest.
- Banks/organisations charge only a small amount of money to offer loans.
- Advised to take loans from well-known and authentic organisations/banks.

9. Insurance fraud

Fraudsters collect the policyholder database from Insurance companies and broking companies, call the policyholders and lure them by telling them about new policies with fake benefits or providing benefits in the name of existing policies.

Precautions:

- Don't trust calls in the name of insurance policies.
- Verify if the caller is from a genuine company before paying the amount.

10. Gift Frauds

Fraudsters operating from Bihar state send BULK SMS/Mails announcing the prize wins in the name of various e-commerce sites such as Snapdeal, Naaptol, Flipkart, Paytm Mall, Amazon, Homeshop, Shopclues, etc. They also share their identity cards as employees of these companies to gain the trust of innocents. Furthermore, they cheat the innocents by collecting

money from them under the guise of Registration Fees, Service Charges, GST, and Processing Fees.

Precautions:

- Do not respond to messages/emails received from unknown persons regarding
- Gift/prize money.
- Do not pay money to unknown in the name of claiming prize money.

11. Dating and Female Escort Fraud

Many fraudsters are looting men in the name of dating sites. To register with these sites, they cite various fee structures and loot in the name of providing a female escort.

Precautions:

Don't fall prey to dating/female escorting sites

Advised not to get registered at different sites like Tinder, etc.

12. Lottery Frauds

A **lottery scam** is a type of advance-fee **fraud** which begins with an unexpected email notification, phone call, or mailing (sometimes including an extensive check) explaining that "You have won!" a large sum of money in a **lottery**.

E.g.,

a. Coca-Cola, Samsung, Microsoft & Tata lottery frauds by Nigerians

b. local lottery fraud in INDIA, such as Snapdeal, Amazon, and Work from Home.

Precautions:

- Never believe any message, including bulk SMS, received on mobile numbers about the offering of prizes, gifts, a lottery, etc.
- Always shop on secure websites, i.e., https://
- Don't believe in the offer/sale of goods at low prices.

13. Matrimonial Frauds

Fraudsters register with matrimonial sites with fake details and sophisticated profiles, mostly targeting well-earning individuals. They then come up with cooked-up stories to loot money.

Precautions:

- Meet the person physically before going into any relationship
- Do not share private information/photos/videos with persons met on these sites.

14. Online Friendship Frauds

Earlier, Nigerians used to create fake Facebook accounts with different display pictures and send requests to other accounts. When somebody accepts a request, they start chatting with them. After a few days, they say they are sending or coming to India with gifts. After a few days, victims receive calls in the name of customs and ask to pay amounts to claim their gifts. In recent days, fraudsters have been creating fake or impostor Facebook and other social media accounts, impersonating individuals and messaging their friends or contacts, requesting money. Many victims are transferring funds without verifying the person.

Precautions:

- Do not accept friend requests from unknown strangers on social media sites and messaging applications.
- Do not believe in fake calls in the name of customs.
- Only transfer funds to others after verifying with the person.

15. Investment Frauds:

The fraudsters are pushing bulk SMS (e.g., AD-JAISTP), offering part-time jobs at Flipkart and Amazon, where one can earn vast amounts of the sum invested by completing simple daily tasks. If anyone responds to the message, fraudsters ask them to join a group on Telegram or social media accounts and share links with them to get registered. Mainly, group admins (foreign ladies) monitor their transactions. Initially, they ask to invest a nominal amount and give tasks to earn a profit. They show profits in virtual wallets and allow the customers to withdraw profit amounts to gain customers' trust. They also offer commissions for referring others and give daily updates on the profits earned. These sites/applications gain popularity through word-of-mouth publicity made by the users. Once fraudsters collect a huge amount, they block the withdrawal process and gradually disable the sites/applications. These criminals also use cold-calling tactics to lure investors and victims by manipulating them into investing.

Advisory:

Do not download applications in .apk format; instead, download only from the Google Play Store.

Do not believe in applications that show profits virtually.

Refrain from trusting investment applications or sites that have emerged or gained popularity quickly.

Do not join groups offering investment tips or ideas on social media applications (WhatsApp/ Telegram).

16. Cyber Crime Against Women:

(Abusive mail/messages and creating fake accounts on social networking websites)

- Culprits collect photographs from social networking sites, morph the photos and post them on porn websites.
- Cheaters collect photograph details and create fake profiles on social networking websites to defame them.
- Collecting the mobile numbers and email ID database and sending abusive and vulgar messages/emails to them.
- Posting the mobile numbers on dating sites and social media.
- Cheating the women by seeing their profiles on the matrimony website, sending interest requests, and collecting money in the name of trust by offering to marry.

Precautions:

- Don't post personal photographs on social networking sites.
- Don't share personal information with unknown or known persons.
- Don't disclose mobile numbers to unknown persons.
- Unless you meet and verify personally, don't trust others and don't share information on matrimony websites.

16A. Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. It has become more common among teens and includes actions to manipulate, tease, troll, harass, and defame any person. A cyberbully is not necessarily a habitual cybercriminal or stranger; sometimes, it could be someone you know. It is mostly about posting negative comments, trolling on social media, or spreading rumours to defame someone.

Precautions:

- Never share your passwords and personal information online.
- Make use of privacy and security settings on social media sites.
- Do not accept unknown friend requests on social media sites.
- Avoid posting explicit photos of yourself online.

16B. Cyber Stalking:

Fraudsters continuously send messages and make abusive posts on social media sites. They also post the mobile numbers of their targets on classified sites.

Precautions:

- Do not accept friend requests from the unknown.

- Enable privacy settings for social media sites.
- Avoid posting explicit photos of yourself online.
- Report fraud if any offensive post or message is found.

16C. Creating fake accounts:

Fraudsters create fake accounts on social media or porn websites, posting photos or mobile numbers of the target, causing harassment and mental agony to their targets.

Precautions:

- Avoid posting explicit photos of yourself online.
- Do not share your personal or sensitive information with anyone.
- Enable security locks or privacy settings on social media accounts.
- Use strong and complex passwords.
- Do not engage in unnecessary discussions or debates online.

17. Corporate Crime (Email ID Hacking):

(Email hacking and Data Theft/Source Code theft)

Culprits collect a database of company-related information, hack email IDs, intercept emails, and transfer funds to their (fraudsters) accounts.

Precautions:

1. Maintain your own websites to prevent email ID hacking.

- While performing financial transactions, verify each letter of the mail ID with the original mail ID and mail header.
- Check the mail source or mail header to find whether mail is routed through the proper
- Confirm the bank account by verifying with the customer through a call before transferring funds channel.

17A. Data Theft:

Collecting and using the company database causes loss to the company.

Company employees, in collusion with other competitors, transferred the database and source code to others, causing considerable losses to the management.

Precautions:

- Take a Non-Disclosure Agreement from employees and don't allow browsing of personal emails and social networking sites. Maintain strong firewalls and anti-virus protection to prevent attacks like DOS attacks, hacking, etc.

*****

NEW CRIMINAL CODES AND THE QUEST FOR EFFECTIVE JUSTICE IN INDIA

Dr. M. V. Chandramathi
Principal
Anantha Law College,
Kukatpally, Hyderabad
Affiliated to Osmania University

I. Introduction

India now stands in middle of deep criminal law transition with three new criminal codes coming into force in 2024 (India's New Criminal Laws,2024).The Bharatiya Nyaya Sanhita 2023,Bharatiya Nagarik Suraksha Sanhita 2023 & Bharatiya Sakshya Adhiniyam 2023 formally replace Indian Penal Code 1860,Code of Criminal Procedure 1973 & Indian Evidence Act 1872 (India's New Criminal Laws,2024).The reform aims to shift system from colonial punitive orientation towards citizen focused,victim centred & technologically enabled model of justice (India's New Criminal Laws,2024).The implementation paper on three criminal laws stresses continuity with constitutional vision of social,economic & political justice under Preamble (Implementation of Three Criminal Laws,n.d.).It presents change as "Indianisation" of criminal justice that still preserves proven provisions of old statutes where they align with constitutional values & practical needs (Implementation of Three Criminal Laws,n.d.).Bhargava & Chaudhary read these developments as part of broader constitutional recalibration of criminal law around Articles 14,19 & 21 (Bhargava & Chaudhary,2025).

II. Colonial Legacy & Imperative of Reform

The Malimath Committee on Reforms of Criminal Justice System identified structural weaknesses long before present overhaul,including weak investigations,low conviction rates & systemic delay (Committee on Reforms of Criminal Justice System,2003).It emphasised that fragmented amendments could not cure deep design flaws in investigation,prosecution & trial processes (Committee on Reforms of Criminal Justice System,2003).The Committee also argued that system ignored victims,encouraged hostility between police & public,and often failed to inspire confidence in fair outcomes (Committee on Reforms of Criminal Justice System,2003). Subsequent scholarship noted that colonial codes did not anticipate cybercrime,organised crime,hate crimes or digitally organised violence & fraud (Trivedi,2025).Trivedi points out that new offending patterns demand greater clarity in definitions & more nuanced sentencing

frameworks than IPC provided (Trivedi,2025).Bhargava & Chaudhary add that colonial laws carried implicit logic of ruling power & public order,rather than logic centred on constitutional citizenship & dignity (Bhargava & Chaudhary,2025).

III. Bharatiya Nyaya Sanhita 2023: Substantive Criminal Law Reform

The Bharatiya Nyaya Sanhita 2023 consolidates & amends offence provisions while presenting itself as core instrument of substantive criminal law (Government of India,2023a).The bare text confirms its objective to consolidate & amend provisions relating to offences & connected matters,effectively taking place of IPC (Government of India,2023a).Trivedi describes BNS as India's "new transformative criminal law",because it attempts to address modern criminal realities while claiming to decolonise legal language & philosophy (Trivedi,2025).The BNS introduces specific offences for organised crime,terrorism & certain forms of mob violence,and it recognises snatching as separate category beyond ordinary theft (Why was BNS 2023 Enacted,2024).The Common Cause article explains that Section 304 BNS defines snatching & enhances punishment in ways intended to respond to street crime concerns,though questions remain about proportionality & necessity (Why was BNS 2023 Enacted,2024).The same article highlights new provision on mob lynching,which criminalises group murder motivated by identity based hatred & prescribes severe penalties,marking explicit legislative response to recurring social violence (Why was BNS 2023 Enacted,2024).At same time,critics argue that promise of "decolonisation" looks limited because many colonial era offence structures remain largely intact,sometimes with harsher punishments (Common Cause Editorial,2024). The Common Cause editorial notes that provisions replacing sedition appear broader & risk converting wide zone of dissent or criticism into criminalised behaviour in name of national security (Common Cause Editorial,2024).Bhargava & Chaudhary also caution that enhanced punishment & wider definitional ranges must be tested against constitutional proportionality & Supreme Court's civil liberties jurisprudence (Bhargava & Chaudhary,2025).

IV. Bharatiya Nagarik Suraksha Sanhita 2023: Procedure,Timelines & Custody

The Bharatiya Nagarik Suraksha Sanhita 2023 replaces Code of Criminal Procedure & reworks procedural law with explicit emphasis on speed,timelines & digital tools (Implementation of Three Criminal Laws,n.d.).The implementation paper notes new mechanisms such as online FIR,zero FIR,electronic communication of processes & more rigid time frames for investigation & trial (Implementation of Three Criminal Laws,n.d.).Bhargava & Chaudhary identify these provisions as part of justice system that aspires to be more efficient & technology driven without formally compromising due process standards (Bhargava & Chaudhary,2025). The Indian Police Journal special edition underlines that BNSS encourages forensic driven investigations by making forensic examination mandatory in serious offences,particularly those with punishment of seven years or more (Bureau of Police Research & Development,2024).It describes capacity building programmes for police & prosecutors to understand new timelines

& digital processes,including e-documentation & audiovisual recording of key procedural steps (Bureau of Police Research & Development,2024).Such measures aim to reduce dependence on oral testimony alone & to shift practice towards scientifically grounded evidence & transparent records (Bureau of Police Research & Development,2024).However,Common Cause editorial flags serious concerns about changes to police custody,because BNSS allows police custody at any time during first 40 or 60 days of detention,rather than only immediately after arrest (Common Cause Editorial,2024).The editorial warns that this flexibility may increase exposure of accused persons to coercion & custodial violence,particularly where internal & external oversight mechanisms remain weak in practice (Common Cause Editorial,2024).Bhargava & Chaudhary similarly stress that tighter timelines must not become justification for cutting corners on fair hearing,legal aid,or reasoned judicial scrutiny of remand & bail (Bhargava & Chaudhary,2025).

V. Bharatiya Sakshya Adhiniyam 2023: Digital Evidence & Truth Finding

The Bharatiya Sakshya Adhiniyam 2023 consolidates rules of evidence for judicial proceedings & explicitly recognises centrality of electronic & digital records (Government of India,2023b).Section 1 states that Act provides general rules & principles of evidence for fair trial,and it applies to all judicial proceedings,including courts martial (Government of India,2023b).The implementation paper highlights that BSA treats electronic records as primary evidence,simplifying admissibility & enabling courts to rely more confidently on digital trails (Implementation of Three Criminal Laws,n.d.).The BPR&D special issue explains that new presumptions & standards for digital evidence intend to secure integrity of electronic material,including metadata,call detail records & other cyber forensics outputs (Bureau of Police Research & Development,2024). It also underlines need for specialised training for investigating officers & prosecutors,so that collection & presentation of electronic records meet statutory & technical requirements (Bureau of Police Research & Development,2024).Bhargava & Chaudhary read these developments as part of State's response to cybercrime & technologically complex offences,where traditional evidentiary concepts struggle to capture full picture (Bhargava & Chaudhary,2025).

VI. Victim Centric & Rights Oriented Justice

Both implementation paper & constitutional analysis by Bhargava & Chaudhary place strong emphasis on victim centric justice (Implementation of Three Criminal Laws,n.d.; Bhargava & Chaudhary,2025).The implementation paper records that new framework introduces community service,enhanced compensation & better information rights for victims at different stages of process (Implementation of Three Criminal Laws,n.d.).It links these features to broader philosophy where punishment should also yield social benefit,not merely inflict suffering on offender (Implementation of Three Criminal Laws,n.d.).The Indian Police Journal notes that victim rights find recognition in procedural obligations to inform victims about investigation progress,charge filing,and trial developments (Bureau of Police Research & Development,2024).

It stresses that improved communication,combined with support services,can strengthen trust in police & courts & encourage cooperation with lawful processes (Bureau of Police Research & Development,2024).Trivedi also comments that BNS,by introducing new offences & refining definitions,attempts to protect vulnerable groups more directly,particularly in cases of hate motivated or identity based violence (Trivedi,2025).From constitutional perspective,Bhargava & Chaudhary link victim centric reforms with right to life & dignity under Article 21 & with equality guarantees under Article 14 (Bhargava & Chaudhary,2025).They argue that effective criminal law should simultaneously respect rights of accused & provide meaningful recognition,participation & protection to victims in line with international standards like ICCPR & UN victim declarations (Bhargava & Chaudhary,2025).

VII. Technology,Digitalisation & Access to Justice

The paper on new criminal laws notes how digitisation,e-filing,e-courts & virtual hearings seek to reduce delay & improve transparency in criminal proceedings (Implementation of Three Criminal Laws,).It explains that e-FIR & zero FIR mechanisms allow complainants to file information irrespective of territorial barriers,using online or electronic communications,including email & other platforms (Implementation of Three Criminal Laws,n.d.).The blog on India's new criminal laws similarly highlights digital integration as core feature designed to support efficiency,accessibility & better record management (India's New Criminal Laws,2024).The BPR&D special issue describes capacity building initiatives to familiarise frontline police with digital reporting tools,audiovisual recording of statements & secure storage of electronic case records (Bureau of Police Research & Development,2024).Such institutional training tries to ensure that promise of digital justice does not remain confined to metropolitan or higher court spaces alone (Bureau of Police Research & Development,2024).Bhargava & Chaudhary also note that technology can promote open courts & public scrutiny,for instance through accessible digital cause lists & online publication of orders,subject to privacy safeguards (Bhargava & Chaudhary,2025).Yet,both academic & policy discussions warn that digital exclusion may create new inequalities if poor,rural or marginalised communities lack access to reliable connectivity,devices or legal assistance (India's New Criminal Laws,2024).The justice system must therefore pair technological innovation with legal aid services,public facilitation centres & language sensitive interfaces,so that reforms genuinely expand access rather than shrink it (Implementation of Three Criminal Laws,).

VIII. Critiques,Concerns & Constitutional Scrutiny

The Common Cause editorial raises fundamental questions about whether new codes truly "decolonise" criminal law or merely repackage colonial structures with Indian names & harsher punishments (Common Cause Editorial,2024).It points out that many colonial provisions remain,and that new laws in some respects broaden reach of State coercive power,particularly in realm of public order & national security (Common Cause Editorial,2024).The same issue's

detailed feature on BNS underlines that provisions replacing sedition have expansive language that may allow prosecution of activities which are otherwise part of democratic dissent (Why was BNS 2023 Enacted,2024).Common Cause further notes that BNS effectively reintroduces substance of Section 303 IPC,concerning murder by life convict,in form of Section 104 prescribing life imprisonment till natural life (Why was BNS 2023 Enacted,2024).The article recalls that Supreme Court in Mithu v.State of Punjab struck down Section 303 for violating Articles 14 & 21 because it imposed mandatory death sentence without judicial discretion (Mithu v.State of Punjab,1983 AIR 473).This background suggests that new provisions with similar severity must undergo careful constitutional review to avoid repeating past defects (Mithu v.State of Punjab,1983 AIR 473).The same Common Cause discussion also refers to Navtej Singh Johar & Ors.v.Union of India,where Supreme Court read down Section 377 IPC & protected consensual same sex relations between adults (Navtej Singh Johar & Ors.v.Union of India,AIR 2018 SC 4321).That decision rested on dignity,privacy & equality,and it demonstrates that criminal law cannot criminalise intimate conduct merely on majoritarian moral grounds (Navtej Singh Johar & Ors.v.Union of India,AIR 2018 SC 4321).Bhargava & Chaudhary therefore argue that any new sexual or morality based offences under BNS must remain consistent with these constitutional principles & with international obligations under instruments like ICCPR & UDHR (Bhargava & Chaudhary,2025).Finally,Malimath Committee report reminds that even best designed laws fail if institutions lack integrity,resources & accountability (Committee on Reforms of Criminal Justice System,2003).The BPR&D materials show efforts to address training & capacity,yet concerns remain regarding political influence,uneven policing standards & access to competent defence counsel (Bureau of Police Research & Development,2024).The quest for effective justice under new codes will therefore depend on continuous monitoring,public engagement & willingness to revisit problematic provisions through democratic processes (Common Cause Editorial,2024).

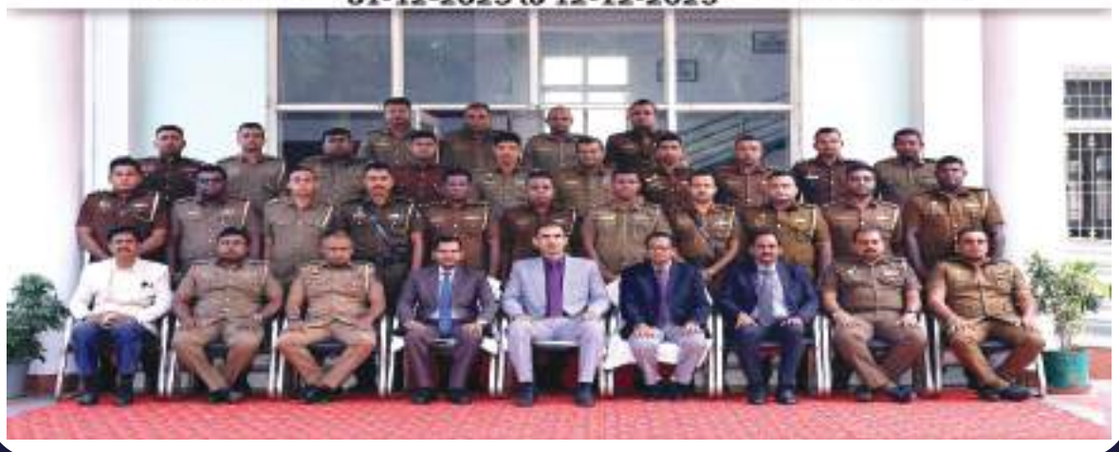
IX. Conclusion

The three new criminal codes seek to modernise Indian criminal law,respond to new forms of crime,strengthen victims' rights & integrate technology into justice process (India's New Criminal Laws,2024).They claim to shift focus from colonial punishment to Indian notions of nyaya grounded in constitutional guarantees of dignity,equality & liberty (Implementation of Three Criminal Laws,n.d.).At same time,informed critiques highlight expanded police powers,ambiguous offence definitions & risk of undermining civil liberties if safeguards do not operate robustly in practice (Common Cause Editorial,2024).Constitutional jurisprudence in Mithu & Navtej shows that criminal law must remain proportionate,non arbitrary & respectful of individual autonomy & dignity (Mithu v.State of Punjab,1983 AIR 473; Navtej Singh Johar & Ors.v.Union of India,AIR 2018 SC 4321).Whether new codes truly advance effective justice in India will finally depend less on their symbolism & more on their day to day implementation by police,prosecutors,defence counsel & judges across country (Bhargava & Chaudhary,2025).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

ITEC/MEA Course for Sri Lankan Police officers on "Handling Crime Investigation"

01-12-2025 to 12-12-2025



CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Advance Scientific Investigation for Royal Bhutan Police officers"

24-11-2025 to 05-12-2025

CENTRAL DETECTIVE TRAINING INSTITUTE HYDERABAD

cdtshyderabad@nic.in
cdtihyd@gov.in
040-27038182, 29704150

@bprdcdtihyd
@bprdcdtihyd
@bprdcdtihyd

Address :
CDTI, Ramanthapur,
Hyderabad,Telangana,
Pin-500013

Editor in cheif : Shri Salmantaj Patil, IPS, Director
Editor : Shri V Bheemakrishna Naik, PA (TRG.)