गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

विद्यया ऽमृतमश्नुते
एन सी ई आर टी
NCERT

Ministry of Education
Government of India
सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

LEGAL WAYS OF HANDLING CYBER THREATS

SH. JITENDER SINGH, ACP, I4C, MHA

INSP. RAKESH DESWAL, I4C, MHA

CYBER CRIME SNAPSHOT

More than 25 Lac Complaints reported till date on National Cyber Crime Reporting Portal (since, August 2019)

Average **4500** complaints reported daily (August, 2023)

Over **10,00,000 suspect** mobile numbers

More than Rs 700 Crores saved using 1930 Cyber Helpline Number

Over 50% crimes reported are cyber financial frauds on NCRP

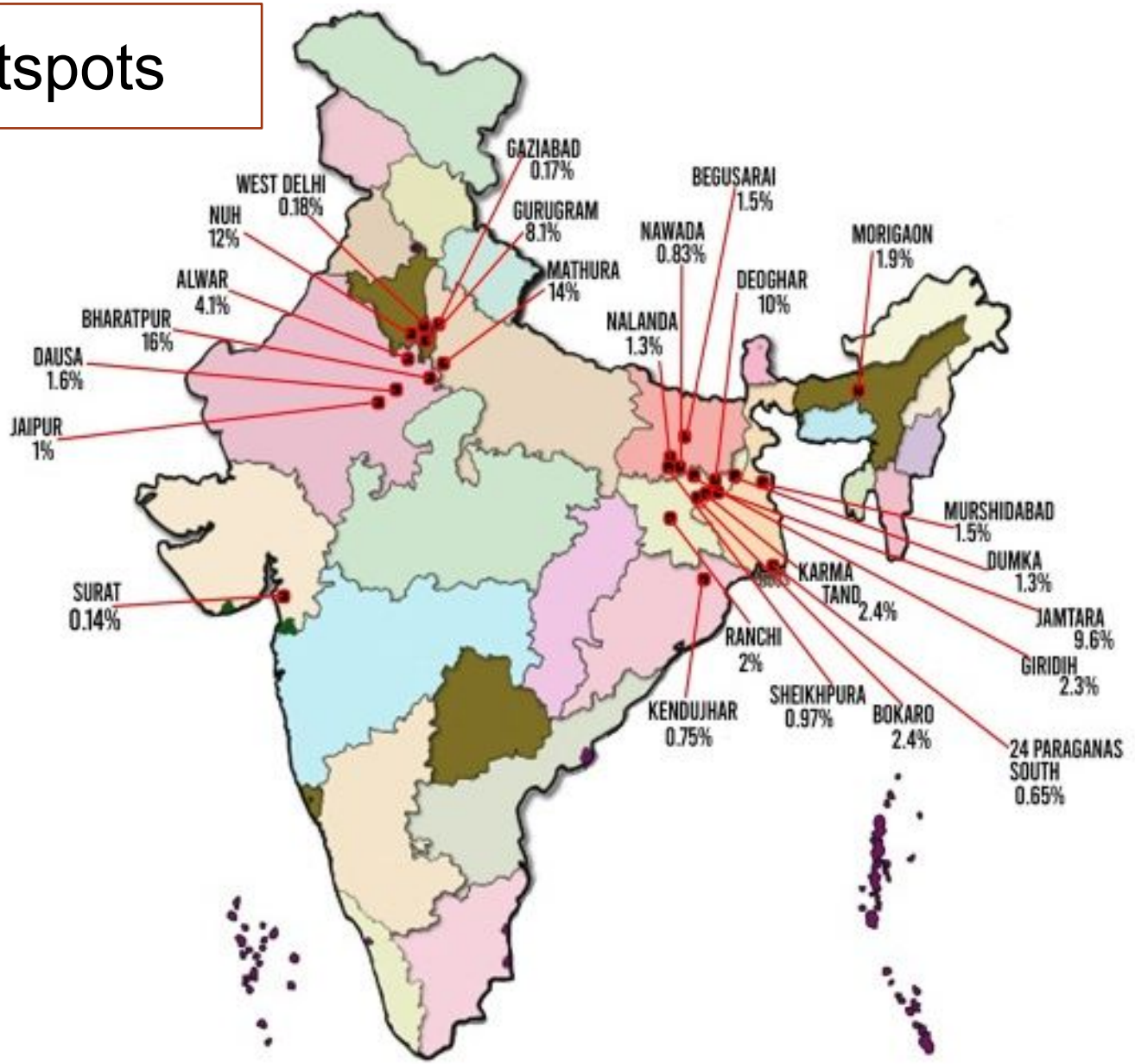
Anonymous Technology – VPN, VoIP, Mule Accounts etc.

1 % to 2% converted into FIRs

Major Cyber Crime Hotspots

1. Bharatpur (16%)
2. Mathura (14%)
3. Nuh (12%)
4. Deoghar (10%)
5. Jamtara (9.6%)
6. Gurgaon (8.1%)
7. Alwar (4.1%)
8. Bokaro (2.4)
9. Karma Tand (2.4%)
10. Giridih (2.3%)

शीर्ष 10 जिलों में 80.9% साइबर अपराध होते हैं



STAKEHOLDERS IN CYBER CRIME

- Computer Emergency Response Team (CERT-IN)
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- Indian Cyber Crime Coordination Centre(I4C)
- Cyber Crime Agencies or Cyber police Stations in States/UTs of India
- T-Soc , Department of Telecommunication
- Reserve Bank of India
- Ministry of Electronics and Technology (MeitY)
- National Payment Corporation of India
- Private, Public and Cooperative Banks etc.,

INDIAN DATA PROTECTION REGIME EVOLUTION

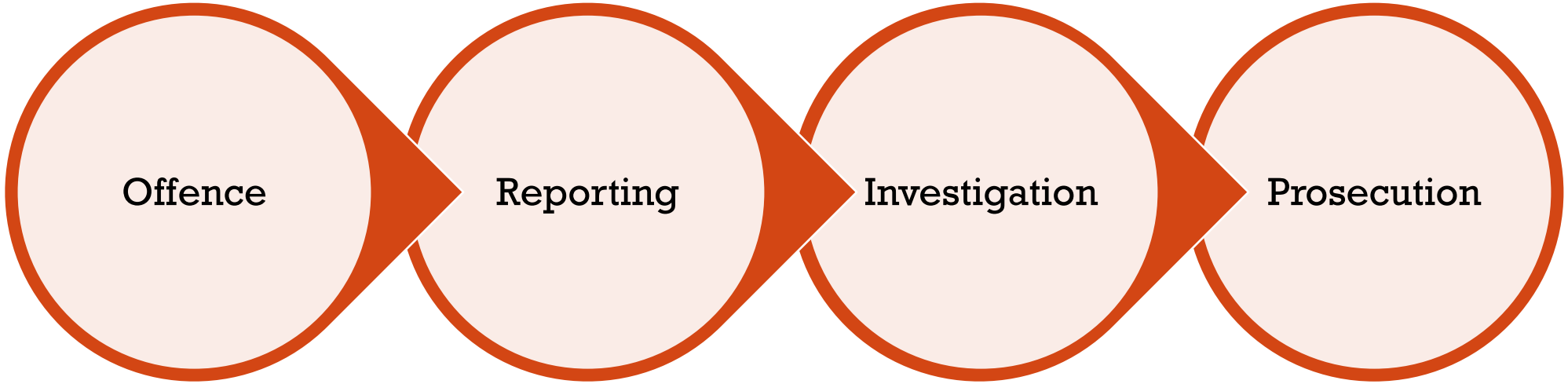
2008	IT (Amendment) Act Privacy clauses
2011	Notification of privacy rules under Sec 43A of IT Amendment Act 2008
2012	Framework by A P Shah Expert Group on Privacy; DoPT draft law
2014	Security-Privacy Framework for Smart Cities
2015	RBI Cyber Security Framework; SEBI Cyber Security Guidelines
2016	Aadhaar Law and Regulations focusing on Privacy; IRDAI Cyber Security Framework
2017	'Right to Privacy' as Fundamental Right
2018	Draft Data Protection Bill & Report by Srikishna Committee; Aadhaar Supreme Court Judgment; Draft Healthcare Act (Disha)
2019	Updated Draft Data Protection Bill Tabled in Parliament; Parliamentary Committee convened Withdrawn-2022
2022	Digital Personal Data Protection(DPDP) Bill 2022
2022	The Draft Indian Telecommunication Bill, 2022,
2023	Proposed Digital India Act , 2023

HOW PI IS USED OR SHARED

HOW PI IS PROTECTED

WHO WOULD BE ACCOUNTABLE FOR ITS MISUSE

CYBER THREAT/CRIME CYCLE



CYBER THREAT CLASSIFICATION

Contravention (Civil wrong)

v/s

Offences (Criminal wrong)

CONTRAVENTION (CIVIL WRONG)

- A cyber contravention refers to a civil wrong under IT Act, 2000.It is important to note that Law of torts provide remedies for civil wrong where affected person can compel the wrong doer to pay damages by way of compensation.

- Section 43A. Compensation for failure to protect data. - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

CONTRAVENTION (CIVIL WRONG)

- Adjudication of Cyber Contraventions –Sec-46-47
- Compensation upto 5 Crore –Adjudication officer
- Appeal-TDSAT(Telecom Disputes Settlement & Appellate Tribunal)
- Civil Courts are barred up to 5 Cr (Sec 61 IT Act)
- More than 5 Cr-Civil Court/High Court

SIM SWAP CASE -Judgements-IT Secretary

OFFENCES (CRIMINAL WRONG)

Section 65. Tampering with computer source documents.
Section 66. Computer related offences.
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device.
Section 66C. Punishment for identity theft.
Section 66D. Punishment for cheating by personation by using computer resource.
Section 66E. Punishment for violation of privacy.
Section 66F. Punishment for cyber terrorism.

OFFENCES (CRIMINAL WRONG)

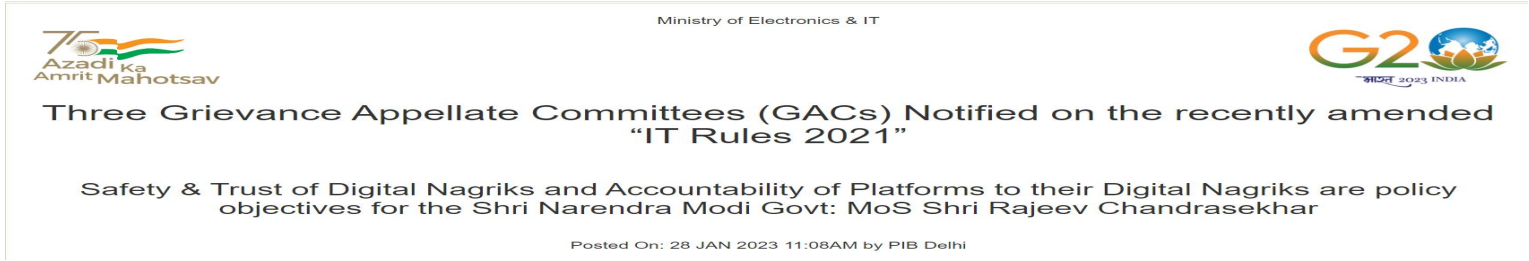
- Section 67. Punishment for publishing or transmitting obscene material in electronic form.
- Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
- Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
- Section 67C. Preservation and retention of information by intermediaries.
- Section 77B. Offences with three years imprisonment to be bailable.
- Section 78. Power to investigate offences.

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021 [UPDATED AS ON 6.4.2023]

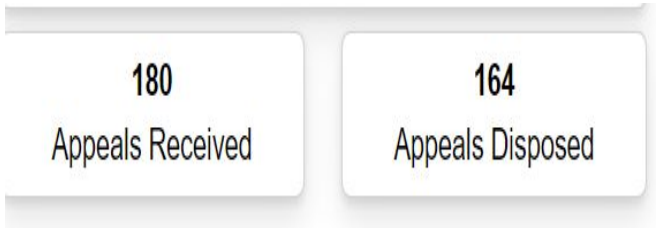
- Rule 3(2) Grievance redressal mechanism of intermediary
- Grievance officer and contact details
- Who can complaint: user or victim
- Grievance officer will acknowledge complaint within 24 hours
- Grievance officer will resolve complaints within 15 days

(If sensitive in nature then in 72 hours)

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021 [UPDATED AS ON 6.4.2023]



- 3A. Appeal to Grievance Appellate Committee(s)
- Appeal against Grievance officer with in 30 days
- GAC will resolve complaints with in 30 days



https://www.gac.gov.in

IMMUNITY

Section 79 of the IT Act talks about certain **exemptions from liability for the intermediaries** in case of any third party information, data, or communication link made available or hosted by them. This exemption would apply in the following cases :

1. Function of intermediary is limited to only providing access to communication system;
2. Intermediaries do not-
   (a) Initiate transmission;
   (b) Select the receiver of the transmission, and
   (c) Modify or select the content contained in the transmission
3. Intermediaries shall exercise due diligence while discharging their duties and also observe to any guidelines which may be prescribed by the Central Government.

LIABILITY

- **Section 79 of the IT Act** further talks about the cases where exemption shall not apply :

- If intermediary has by **threats or promise or otherwise, conspired, abetted or induced in commission of an unlawful act**,

- **TAKE DOWN NOTICE** –79.3(b) IT Act

(b)upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Shreya Singhal Vs UOI(2015)

WAYS TO REPORT CYBER CRIMES

- Immediately call 1930 (if financial fraud) or report at www.cybercrime.gov.in in all cyber related offences
- Visit your nearest Cyber Crime or local Police station
- Write to Bank and RBI Ombudsman (RBI Limited Liability Guidelines 2017)
- Report to Grievance Officer of related Social Media Intermediary through their channel in case of any unauthorised access/hack/removal etc.
- Appeal to Grievance Appellate Committee at www.gac.gov.in against the Grievance Officer action, if not satisfied.

AWARENESS IS KEY

Follow *CyberDost* on social media

- Get the latest Cyber Safety Tips
- Learn about various types of Scam Alerts
- Get updates on National and International Cyber news
- Learn about the achievements in the attempt to make the nation cyber safe
- Become a Cyber Volunteer and share the CyberDost content with your community
- Do your bit to stay vigilant and stay cyber safe!

@cyberdosti4c @CyberDosti4c @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c @cyberdost @cyberdost

Q & A