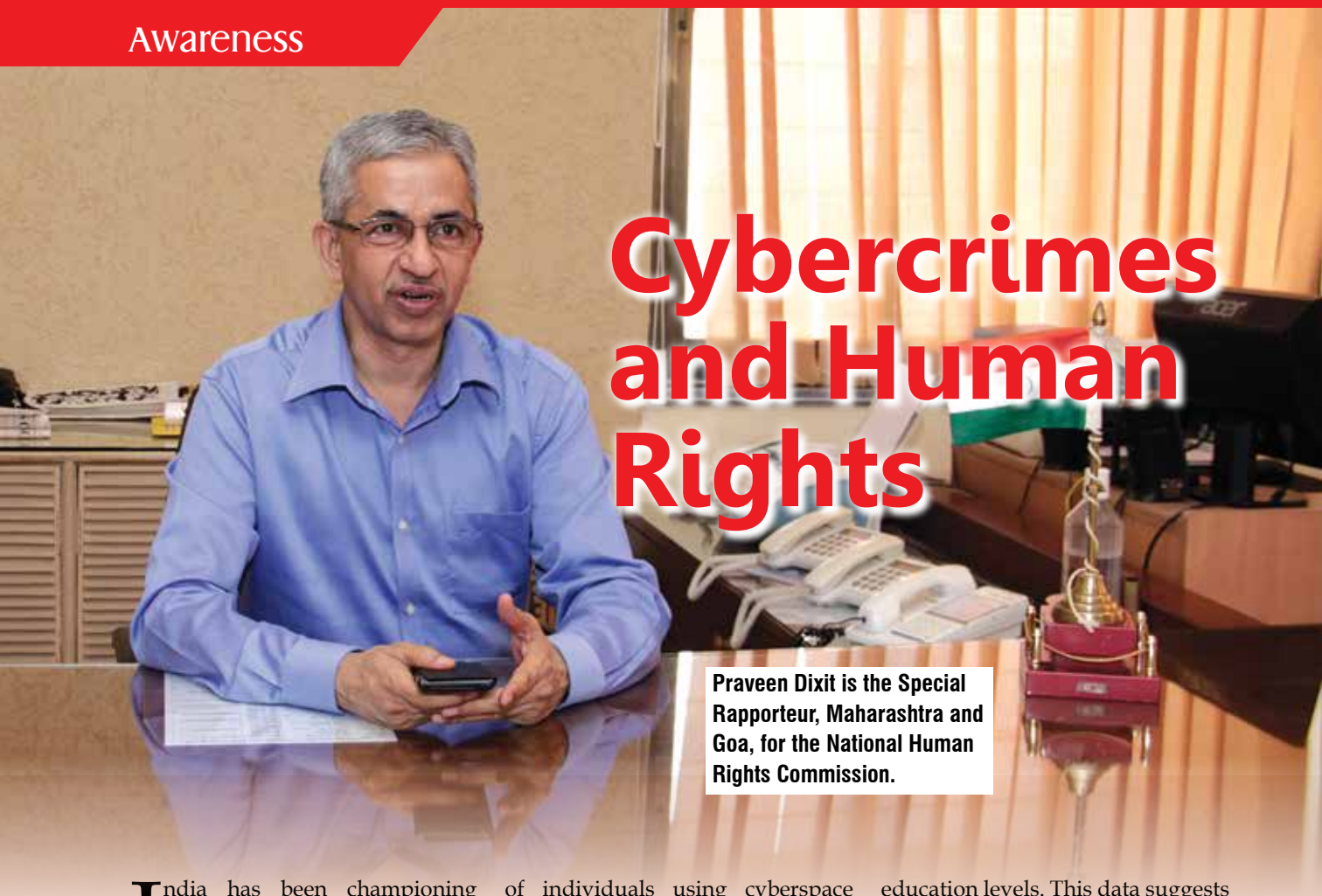


Cybercrimes and Human Rights

Praveen Dixit is the Special Rapporteur, Maharashtra and Goa, for the National Human Rights Commission.

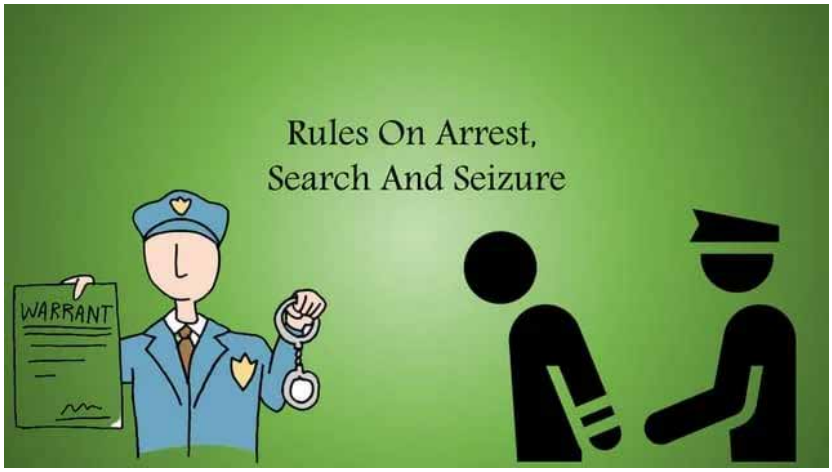
India has been championing human rights for centuries and applying the same principles to not only individuals but also the rights of animals, birds, marine creatures, and the natural world, including mountains, trees, rivers, and oceans. This is achieved through the implementation of the Indian Constitution, which outlines enforceable fundamental rights and provides Directive Principles to steer State Policy. This has been further strengthened through the establishment of National and State Human Rights Commissions from 1993 onwards. While these efforts witnessed great success, the last two decades have noticed technological innovations in the field of information, technological revolution and communication. It is believed the number of persons using computers and mobiles in India is nearly one billion and the same is likely to witness further escalation in the coming years with increasing speed. As the number of individuals using cyberspace grows, so does the presence of anti-social elements who exploit legal, economic, and social vulnerabilities, often infringing on the human rights of many. Data from the National Crime Records Bureau (NCRB) reveals that cybercriminals target people of all ages, including infants, young children, adolescents, young adults, and the elderly, spanning across all socioeconomic backgrounds and education levels. This data suggests that virtually no one is immune to this pervasive threat.

India has been sensitive to these ever-expanding threats from the cyber world and endeavours to undertake all possible measures to combat the same through international, national, legal, and organisational efforts by adopting innovative technologies from time to time. The first step in this

direction was the adoption of the Information Technology Act 2000 (IT Act), with Amendments in 2008, and 2015.

To ensure cyber security, there are five main types of laws followed in India. These include the Information Technology Act 2000, (IT Act), Bharatiya Nyaya Sanhita, 2023, (BNS), the Information Technology Rules (IT Rules), the Companies Act of 2013 and the Cybersecurity Framework (NCFS). These highlight penalties and sanctions enacted by the Parliament of India that safeguard the sectors of e-governance, e-banking, and e-commerce.

In a major step to repeal archaic three criminal laws, the Parliament adopted Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam 2023, and the same have been implemented throughout the country from July 1, 2024. These enactments expressly recognise electronic communication as approved in the criminal process and thereby promote transparency. These also ensure the rights of victims. Moreover, the earlier practice of inordinate



delays causing enormous harm to the cause of justice has been curbed through timelines for the entire process. Cyber offences through electronic devices have been expressly mentioned along with penalties to protect children, women, and elderly persons in the beginning chapters of BNS. The human rights of individuals during arrest, searches and seizures have been well protected through mandatory video recording of the entire process. To ensure details of persons who are missing or disappearing, the BNSS has made it mandatory for every police station and district police headquarters to display details of arrested persons including the name of the arrested person, charges, time, etc., digitally. It is also mandatory to have forensic experts examine a person when the offence is punishable for more than seven years.

To curb the nefarious practice of determining the sex of the foetus, sonography machines were being used widely. India has promulgated the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act 1994 along with initiating a movement called Beti Bachao, Beti Padhao throughout the country. This has reduced female infanticides and helped to improve the male-female sex ratio considerably.

Cybercriminals are increasingly exploiting cyberspace to promote terrorism and recruit young people into extremist ideologies. They leverage the dark web, cryptocurrency, and drug trafficking to further their illegal operations. In response, India has taken a firm stance against all forms of terrorism, maintaining a zero-tolerance policy towards drug trafficking and resisting the legalisation of cryptocurrency to curb such activities. Similarly, India implemented the demonetisation of high-value currency notes to combat counterfeit currency and curb the flow of black money, significantly safeguarding the economic rights of its citizens. To reinforce these efforts, India has amended the Unlawful Activities (Prevention) Act and empowered the National Investigation Agency (NIA) through amendments, allowing them to investigate such offences as federal crimes. In this connection, it is worth recalling the NIA statement on October 10, 2024. It read, "NIA investigations have revealed that five persons were involved in trafficking vulnerable Indian youth to the Golden Triangle Region in Lao PDR where they were forced to commit cyber scams targeting European and American citizens. They operated through the consultancy firm, All International Services, which functioned as a front for human trafficking." (The Perfect Voice, Oct 11, 2024). Increasingly, cybercriminals from China and Pakistan are indulging in cybercrimes against vulnerable Indians, Americans, Australians and British citizens. This underlines the need to have close cooperation among international law-enforcing agencies through multilateral cooperation.

To raise awareness about cybercriminals and encourage best practices for combating them, the National Human Rights Commission regularly issues advisories on technological advancements related to the rights of children, women, the elderly, prisoners, and other vulnerable groups. Additionally, the Commission investigates individual complaints regarding human rights violations to ensure justice at the local level. In addition, the Reserve Bank of India (RBI), along with public and private banks, actively educates customers and the general public on the importance of safeguarding their account details and avoiding fraudulent schemes or reward-based scams. They have widely publicised helplines for early reporting by victims. The Government of India has also set up a dedicated helpline number, 1930, and encourages reporting of cybercrimes through the portal https://www.cybercrime.gov.in, to ensure timely assistance and intervention.

The Department of Telecommunication has a portal called Chakshu to report suspected fraud and unsolicited commercial communication received within the last thirty days - https://services.india.gov.in/service/detail/chakshu-report-suspected-fraud-communication It helps you in several ways, including, Knowing your wireline internet service provider - https://services.india.gov.in/service/service_url_redirect?id=MjQ0MTA=

Reporting incoming international calls with an Indian number- https://services.india.gov.in/service/service_url_redirect?id=MjQ0MDg=

Agency

Knowing the number of connections issued in your name - https://services.india.gov.in/service/service_url_redirect?id=MjQwNTA=

Facility to verify mobile device using IMEI number - https://services.india.gov.in/service/service_url_redirect?id=MjQwNDg=

India Cybercrime Coordination Centre

The Indian Cybercrime Coordination Centre (I4C) was established by MHA, in New Delhi to provide a framework and ecosystem for Law Enforcement Agencies (LEAs) for dealing with cybercrime in a coordinated and comprehensive manner.

I4C - https://i4c.mha.gov.in/ - is envisaged to act as the nodal point to curb Cybercrime in the country. It deals with efforts to create awareness through training law enforcing agencies in 'Cyber Yodha' (https://www.cyberyodha.org/) and has trained thousands of police officers in cybercrime. It also spreads awareness messages through social media in the form of 'Cyber Dost' (https://dot.gov.in/banner/cyber-dost).

According to the website - https://i4c.mha.gov.in/ - safe practices to prevent cybercrime include avoiding pop-ups, unknown mails and links, usage of strong password and authentication, installation of updates and backups for your data.

The portal mentions cybercrime categories such as:

1. Cryptocurrency Crime
2. Cyber Terrorism
3. Hacking/damage of computer systems
4. Online and social media-related crimes such as:

(a) Cheating by Impersonation

(b) Cyber Bullying/Stalking/Sexting

(c) E-Mail Phishing Fake/Impersonating Profile

(d) Impersonating Email

(e) Intimidating Email

(f) Online Job Fraud

(g) Online Matrimonial Fraud

(h) Profile Hacking/Identity Theft

(i) Provocative Speech for Unlawful Acts

To strengthen efforts in fighting cybercrime, the Government of Maharashtra has recently established Cybercrime Investigation Capacity Centre. It claims to possess the best global technologies including Technology Assisted Intelligence (TAI) and machine learning tools to aid investigations into crimes like cryptocurrency fraud and combat cybercrime effectively. It houses the Security Operation Centre (SOC) for the security of the Cyber Security Project. This is designed to manage large-scale security breaches and respond to threats targeting individuals and businesses. It has launched a new dedicated helpline – 14407 - in a 24x7 Command Centre. It has a Computer Emergency Response Team (CERT) to coordinate swift responses to cyber incidents.

I would like to conclude by observing that the right to disconnect one's posts from social media and the right to privacy of personal data are areas which need to be looked into by India urgently. These areas are being misused by cybercriminals extensively. While these efforts by India are laudable, I would urge everyone using cyberspace via computer, mobile or any other electronic device, to completely refrain from responding to any audio or video calls or emails from unknown numbers or email IDs from India or abroad. In case one wants to respond, it is advisable to verify the details of the person calling or emailing. Constant awareness alone can protect your human rights pertaining to life, money, dignity and reputation from the ever-increasing cybercriminals.