Comparative Analysis of AI and Cybercrime Regulations: India and Global Jurisdictions

Authors: Krishna CV Grandhi, Chandra Lekha

As artificial intelligence becomes more nuanced and utilized for varied cybercrimes across nations, countries are rapidly evolving their legal frameworks to stay at pace with the emerging online crimes. Countries are recognizing the need to proactively develop legislations and train regulatory bodies to combat AI-driven crimes. However, in comparison, India's legislative reaction to cybercrimes has been largely reactive with primary criminal statutes lacking proper provisions to address cybercrimes. Jurisdictions like the European Union (EU), United Kingdom (UK) and the United States (US) have undertaken structured, forward-looking approaches in dealing with cyber-crimes.

European Union:

The EU's Artificial Intelligence Act is the world's first comprehensive legal framework designed specifically for the purpose of dealing with artificial intelligence systems and offences. It introduces a novel risk-based classification system that classifies AI systems from minimal to high risk. The framework prohibits high risk systems such as social credit scoring systems and biometric surveillance systems, especially in public spaces. It also mandates strict transparency requirements for AI systems in order to combat the increasing instances of cybercrimes which impact the safety and rights of citizens.

In addition to the AI Act, the EU also consists of the General Data Protection Regulation (GDPR) which provides strong protections against all AI-related privacy violations. The GDPR mandates explicit consent from individuals thereby ensuring that any privacy data breach may be challenged both by individuals and the government. Lastly, the Digital Services Act (DSA) also compels platforms and AI-systems to implement content moderation systems and mandates algorithmic transparency from social media behemoths. Any breach of the conditions laid down under the DSA result in immediate removal of such content. This allows the EU to stay atop of the issues of deepfakes and online impersonation which remain some of the most prevalent AI-driven crimes.

United States:

While the US does not consist of a federal AI legislation, it follows a multi-pronged approach which combines executive action, regulatory enforcement along with guidance and inputs from industry stakeholders. The Federal Trade Commission (FTC) actively investigates and penalizes entities for deceptive AI practices which include instances of deepfakes and impersonation frauds. In addition to actions by the FTC, President Biden's 2023 Executive Order on AI directs federal agencies to develop mandatory AI safety standards which include watermarking synthetic content and clear accountability mechanisms for AI developers.

Lastly, the National Institute of Standards and Technology (NIST) AI Risk Management Framework consists of an actionable guide for public and private sector companies to development reliable AI systems with an emphasis on risk assessment, continuous monitoring and transparent governance and redressal frameworks.

United Kingdom:

The UK, in 2023 has introduced the Online Safety Act specifically addressing AI cybercrimes and imposes legal duties on platforms to identify and remove deepfakes, impersonating content in a swift and timely manner. The National Cyber Security Centre also monitors all cybersecurity threats and sector-specific authorities like the Financial Conduct Authority oversees all AI systems in industries such as banking and insurance.

The UK consists of mandatory risk assessment requirements for companies introducing AI-systems, particularly systems which may impact individual rights and public safety. The risk assessment frameworks provide legal redressal solutions for victims of cyber-crimes such as hacking, deepfakes etc.

China

Despite being one of the most heavily surveyed jurisdictions, China has introduced comprehensive regulatory frameworks to combat cybercrimes. The Regulation on Deep Synthesis Technology of 2023 criminalizes the creation and distribution of deepfakes and mandates labelling or watermarking of AI-generated content. The regulation includes mandatory real-name identification and authentication for internet content creators in order to combat the issue of anonymous distribution of AI content. Any breach of the regulation results in strict liability for platforms hosting such malicious material.

Enforcement Gaps in India

Beyond statutory shortcomings, one of the crucial challenges faced in India are institutional and enforcement gaps in addressing AI-driven cybercrimes. India lacks dedicated regulatory agencies specializing in combating AI-driven cybercrimes. The existing agencies often lack the resources to keep pace with the fast development of artificial intelligence and the training to address issues like synthetic content creation and distribution.

While entities such as the Computer Emergency Response Team India (CERT-In) play a vital role in incident response for cybercrimes, its mandate does not extend to AI-driven crimes such as social engineering attacks, synthetic content creation and algorithmic bias. This has led to a regulatory lacuna for the fast-emerging AI-enabled cybercrimes.

Central agencies like the Central Bureau of Investigation (CBI) and National Investigation Agency (NIA) lack adequate training to combat the technical complexities of AI-driven cybercrimes. Cybercrimes using voice cloning, identity fraud or social media manipulation requires in-depth knowledge on AI-systems, updated

investigation protocols and relevant forensic expertise which remain lacking within the current legal framework.

A comparative analysis between various jurisdictions shines light on the stark disparity in the reactionary pace of addressing AI-driven cybercrimes. While other nations are constructing integrated legal systems which anticipate AI-driven crimes to build preventive mechanisms, India's current system remains ill-equipped to address the vast landscape of AI-driven crimes. India currently requires fundamental reforms like AI dedicated legislations, specialized regulatory agencies with adequate training and expertise and frameworks to establish platform accountability ensuring individual rights. In the absence of such changes, India may risk becoming increasingly vulnerable to AI-driven cybercrimes which continue to evolve and proliferate thereby endangering both public and national security.

www.csail.org