"Obviously, the highest type of efficiency is that which can utilize existing material to the best advantage."
-Jawaharlal Nehru

RAILWAYS SET BENCHMARK

In the modern era of rapid globalization and technological innovation, railways have emerged as a symbol of efficiency, reliability, and sustainable development. Once considered merely a mode of transportation, rail networks today are shaping economies, enhancing connectivity, and setting global standards. India, with its ambitious modernization initiatives and strategic infrastructure projects, has positioned its railway system as a model for the world, demonstrating how effective planning, technology adoption, and policy support can transform a critical public utility into a global benchmark.

Railways are no longer confined to moving passengers and goods. They are catalysts for economic growth, fostering regional development and providing an ecosystem for ancillary industries. The introduction of high-speed trains, semi-high-speed corridors, and modern freight solutions has not only reduced travel time but also improved reliability and service quality. For instance, India's recent initiatives like the Vande Bharat Express, advanced freight corridors, and digital ticketing platforms have set new standards in operational efficiency and passenger comfort, comparable to the best in the world. Such advancements reflect a deep commitment to integrating cutting-edge technology with public service.

Another key aspect that positions railways as a global benchmark is sustainability. Rail transport is inherently more energy-efficient and environmentally friendly compared to road or air travel. Governments worldwide are increasingly looking at electrification, renewable energy integration, and green stations to reduce carbon footprints. India's railway electrification drive, aiming to achieve net-zero carbon emissions by 2030, not only supports climate goals but also sets an example for developing nations striving to balance infrastructure growth with environmental responsibility.

Moreover, the social impact of railways cannot be understated. By connecting remote regions, facilitating trade, and providing affordable mobility, railways contribute to social inclusion and equitable development. They create employment opportunities, enable educational access, and strengthen healthcare delivery through improved connectivity. The alignment of rail projects with broader economic and social policies has enhanced their relevance, making them indispensable instruments of national progress.

Railways are also demonstrating resilience in the face of challenges. During the COVID-19 pandemic, Indian Railways played a critical role in transporting essential goods, medical supplies, and migrant workers, showcasing operational adaptability and logistical prowess. This crisis response highlighted how a well-organized railway system can become a lifeline for millions, earning global recognition for its scale, coordination, and efficiency.

The transformation of railways into a global benchmark is not merely a technical achievement but a testament to strategic vision, innovation, and societal impact. By integrating modern technology, sustainability, and inclusive growth, railways are redefining mobility standards. They are proving that when infrastructure is leveraged thoughtfully, it can become a powerful driver of national prosperity and a model for the world. As countries observe India's achievements, railways stand as a shining example of how transport systems can evolve into engines of progress and global inspiration.

India's Digital Boom and the Shadow Economy of Online Scams

■ **BAIRAJ CHAWALGAMI**

India's meteoric rise as a digitally empowered nation stands as one of the most transformative developments of the 21st century. With rapid proliferation of smartphones, ubiquitous internet connectivity, and ambitious initiatives such as Digital India, the country has ushered millions into the virtual ecosystem of online banking, e-commerce, digital governance, and social networking. However, this unprecedented digital expansion has simultaneously engendered a sinister and insidious phenomenon-online scams and cyber frauds, which have evolved into a formidable socio-economic and psychological menace. Online fraud in India is no longer an episodic aberration; it has metamorphosed into a systemic threat, exploiting technological illiteracy, regulatory lacunae, and human vulnerabilities with alarming sophistication. From phishing expeditions and identity theft to investment rackets and deepfake-enabled impersonations, cybercriminals operate with impunity, often remaining elusive to law enforcement agencies constrained by jurisdictional and technological limitations. The typology of online scams in India is vast and continually mutating. Traditional frauds such as lottery scams and fraudulent phone calls have now been eclipsed by highly nuanced cyber deceptions. Phishing emails masquerading as communications from banks or government agencies lure unsuspecting victims into divulging confidential credentials. Smishing (SMS phishing) and vishing (voice phishing) further amplify this threat, exploiting trust and urgency to precipitate financial losses. More pernicious are investment scams, wherein fraudsters promise exorbitant returns through fictitious cryptocurrency ventures, forex trading schemes, or pseudo-startups. These scams prey on aspirations of quick wealth, particularly among the youth and middle class, culminating in catastrophic financial devastation. Matrimonial frauds, job offer scams, and fake loan apps have also emerged as dominant vectors of exploitation, disproportionately affecting women, students, and economically vulnerable populations.

At the core of online fraud lies psychological subjugation rather than mere technological trickery. Cybercriminals meticulously engineer scenarios that induce fear, greed, or misplaced trust. Posing as law enforcement officials, bank executives, or tax authorities, scammers weaponize intimidation and urgency, compelling victims to act irrationally under duress. The rise of deepfake technology has exacerbated this menace. Fraudsters now manipulate audio and video to impersonate senior executives or family members, rendering traditional methods of verification obsolete. Such hyper-realistic fabrications erode trust in digital communication itself, creating a climate of paranoia and uncertainty. The ramifications of online scams transcend individual financial loss; they inflict macroeconomic and societal damage. Billions of rupees are siphoned annually, undermining consumer confidence in digital transactions and impeding India's ambition of becoming a cashless economy. Small businesses, startups, and rural users-often lacking cybersecurity awareness-bear a disproportionate brunt of these frauds. Moreover, victims frequently endure profound psychological trauma, marked by shame, anxiety, and social stigma. Many refrain from reporting incidents due to fear of ridicule or bureaucratic inertia, allowing perpetrators to operate unchallenged. This culture of silence further entrenches cybercriminal networks. Despite legislative frameworks such as the Information Technology Act, 2000, enforcement remains fraught with challenges. Cybercrime is inherently transnational, with perpetrators often operating from foreign jurisdictions using anonymized networks and cryptocurrency channels. The pace of technological evolution far outstrips the capacity of regulatory mechanisms, rendering many laws obsolete or inadequately enforced. Law enforcement agencies grapple with resource constraints, insufficient training, and overwhelming caseloads. While cybercrime cells have been established across states, their efficacy varies widely. Coordination between banks, telecom providers, and law enforcement is frequently fragmented, allowing critical response windows to lapse. A critical contributor to India's cyber vulnerability is the asymmetrical growth of digital access and digital literacy. While millions have gained internet connectivity, a significant proportion lack foundational knowledge of cybersecurity hygiene. Concepts such as two-factor authentication, secure passwords, and data privacy remain alien to vast segments of the population.Rural and elderly users, in particular, are disproportionately targeted due to their limited familiarity with digital interfaces. The absence of vernacular cybersecurity education further compounds the problem, as most awareness campaigns are confined to English or urban-centric narratives.

Combating online scams necessitates a holistic and multipronged strategy. First, regulatory frameworks must be dynamically updated to address emerging technologies such as artificial intelligence, deepfakes, and decentralized finance. Swift adjudication and stringent penalties are imperative to establish deterrence. Second, financial institutions and digital platforms must assume greater accountability. Proactive fraud detection systems, real-time transaction alerts, and simplified grievance redressal mechanisms can significantly mitigate losses. Collaboration between public and private stakeholders is indispensable. Third, mass-scale digital literacy campaigns must be institutionalized, transcending urban confines and linguistic barriers. Cyber hygiene education should be integrated into school curricula and community outreach programs, empowering citizens to identify and resist fraudulent tactics. Finally, victims must be encouraged to report cybercrime without fear or stigma. A robust, empathetic support ecosystem can dismantle the culture of silence and enable law enforcement agencies to disrupt organized fraud networks effectively. Online scams and frauds represent a dark underbelly of India's digital revolution-a paradox wherein technological empowerment coexists with unprecedented vulnerability. If left unchecked, this menace threatens not only financial security but also public trust in the digital ecosystem. India's aspiration to be a global digital powerhouse hinges on its ability to fortify cyber resilience, foster informed citizenship, and dismantle the shadow economy of cybercrime. The battle against online fraud is not merely technological; it is moral, educational, and institutional. Only through collective vigilance and systemic reform can India safeguard its digital future from the predations of cyber deception.

AI, Digital Arrests and Deepfakes: The Dark Side of the Digital Age

■ **SHALEEN MAHAJAN**

India's rapid digital growth has changed governance, banking, and communication, making services faster, easier to access, and better connected. But this technological progress has also opened the door to complex cybercrimes that take advantage of fear, trust, and differences in digital knowledge. Among the most serious threats are "digital arrest" scams and AI-powered deepfakes, which put basic rights like personal freedom, dignity, privacy, and trust in institutions at risk.

Imagine getting a phone call from someone claiming to be a police officer, warning you that you will be arrested soon, and asking for immediate payment to avoid it. This is not a story and is the reality of digital arrest scams in India. Recent high-profile cases show how serious the problem has become. Bollywood actor Suniel Shetty got temporary protection from the Bombay High Court after his image was misused in deepfake content, while industrialist S.P. Oswal lost ?7 crore to scammers pretending to be the Chief Justice of India and holding a fake Supreme Court hearing. These examples show that digital crimes can affect anyone, regardless of their social status or profession.

A "digital arrest" is a fake scheme used by cybercriminals who pretend to be police officers and force people to make immediate digital payments. Victims are often accused of serious crimes like money laundering or drug trafficking and pressured to pay "verification fees" or "bail money" under threats of arrest, frozen bank accounts, or public embarrassment. Under the Constitution, Article 21 protects personal freedom, while Article 22 guards against illegal arrest. Laws like the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, require proper legal procedures and judicial approval for all arrests. Since a digital arrest has no legal standing, any such demand is a crime, showing a clear mix of fraud, impersonation, and violation of constitutional rights.

"In addition to these scams, AI-powered deepfakes create another serious problem by attacking credibility itself. Generative AI makes non-consensual intimate images (NCII), also called revenge porn, even more harmful by creating hyper-realistic images and videos where someone's face is placed on sexual content, even if no real recording exists. The line between real and fake becomes blurred, making it very hard to prove the content is false. Global studies indicate nearly 90% of deepfake content is pornographic, mostly targeting women. In India, the real scale of the problem is likely higher than official statistics suggest due to social stigma and under-reporting, highlighting the urgent need for both legal and technical solutions.

The term "deepfake" comes from "deep learning" and "fake," and refers to content created using advanced AI techniques like Generative Adversarial Networks (GANs). GANs use large sets of a person's images or videos to make highly realistic copies. Deepfakes can lead to identity theft and fraud. For example, a video falsely showing the MD and CEO of the National Stock Exchange promoting stock services was shared on social media. They also invade privacy and can cause social, economic, and political problems, even affecting democracy, as in the case of Irish presidential candidate Catherine Connolly, who filed a complaint about a fake video claiming she had withdrawn from the election.

In India, the Ministry of Electronics and Information Technology (MeitY) has suggested changes to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These changes require digital platforms to remove banned content once they are aware of it, improve grievance procedures, and label AI-generated or altered content. Platforms must also take care to prevent illegal content from being shared or hosted.

The Information Technology Act, 2000 addresses cybercrimes through multiple provisions. Section 66C punishes electronic identity theft with up to three years imprisonment and a monetary fine. Section 66D penalizes cheating by personation using a computer resource, also with up to three years imprisonment. Section 66E handles privacy violations, while Sections 67 and 67A regulate the circulation of obscene or sexually explicit content. Section 69A empowers the government to block public access to unlawful online content.

The Digital Personal Data Protection Act, 2023 (DPDP Act) requires data fiduciaries to obtain consent from data principals and implement technical safeguards, imposing penalties for non-compliance. The Bharatiya Nyaya Sanhita (BNS), 2023, criminalizes spreading misinformation causing public mischief (Section 353) and allows prosecution of organized cybercrimes, including deepfake-related offences (Section 111). Constitutionally, Article 21 guarantees life and personal liberty, including privacy and dignity, while Article 19(1)(a) protects freedom of speech, subject to reasonable restrictions for public order, decency, morality, and individual dignity.

The concept of safe harbor, provided under Section 79 of the Information Technology Act, 2000, protects intermediaries from liability for actions of third parties, as long as they follow due diligence and do not have actual knowledge of illegal content. Courts have repeatedly emphasized the need to maintain a balance between regulation and freedom of speech. In Shreya Singhal v. Union of India (2015), the Supreme Court struck down unclear and broad powers that allowed the government to block online content without proper safeguards. Similarly, in Kunal Kamra v. Union of India (2020), concerns were raised over granting the Public Information Bureau the power to identify false information, as this could lead to excessive government control and weaken safe harbor protections.

India has also developed several reporting and enforcement mechanisms. The National Cyber Crime Reporting Portal enables anonymous reporting of offences, especially crimes against women and children. The Indian Cybercrime Coordination Centre (L4C) monitors trends and issues notices, while the Sahyog Portal streamlines notice-sharing with intermediaries. CERT-In issues cybersecurity advisories, and the Grievance Appellate Committee hears appeals against decisions of social media grievance officers. In addition, Standard Operating Procedures under the IT Rules, 2021 guide intermediaries and law enforcement agencies in preventing the spread of non-consensual intimate images and deepfakes.

AI-generated content increasingly violates personality rights, as seen in cases such as Arijit Singh v. Codible Ventures LLP, Ankur Warikoo v. John Doe, and incidents involving actor Akshay Kumar. These cases highlight how AI tools are misused to replicate voices, faces, and identities without consent. Recognising these risks, several countries have introduced AI-specific legal safeguards. Denmark has amended its copyright law to protect an individual's body, facial features, and voice for up to 50 years after death. In the United States, the TAKE IT DOWN Act 2025, criminalises the publication of intimate images without consent, including AI-generated deepfakes. China requires both explicit and implicit labelling of AI-generated content, while the EU AI Act (Article 50) mandates that providers and users of AI systems clearly mark synthetic outputs in a machine-readable and detectable form.

In contrast, India's legal framework dealing with cybercrime and artificial intelligence remains fragmented and insufficient. While existing laws punish offences such as obscenity, voyeurism, and cyberstalking, they do not clearly recognise deepfake creation, AI-driven impersonation, or purely digital harms as distinct offences. This gap makes investigation difficult, weakens deterrence, and delays justice for victims. The technical complexity of AI systems, especially Generative Adversarial Networks, further complicates accountability by spreading intent across developers, deployers, and users. As a result, establishing mens rea, verifying digital evidence, and fixing legal liability becomes challenging. Although preventive measures such as MeitY's 24-hour takedown SOP for NCII and deepfakes, on-device deepfake detection by companies like Gen (Norton) and Intel, and biometric liveness systems used in corporate environments show progress, these efforts remain scattered and fall short of a comprehensive legal framework.

Globally, intermediaries are no longer granted absolute immunity. Indonesia's action against Grok AI demonstrates that liability can arise where AI-related harm is foreseeable. Similarly, the EU AI Act follows a risk-based regulatory model with enforceable penalties, in sharp contrast to India's advisory-driven approach. While the Digital Personal Data Protection Act focuses on consent-based data processing, it does not address synthetic or AI-generated representations, leaving victims without effective remedies. Moreover, AI-driven harms such as predictive policing and automated forensic tools challenge traditional ideas of human intent and responsibility under the IT Act, the Bharatiya Nyaya Sanhita, and the DPDP Act, raising serious constitutional concerns under Articles 14 and 21 related to fairness, dignity, and personal autonomy.

AI-generated evidence also presents new challenges for criminal justice. The use of opaque, "black-box" AI tools for risk assessment or forensic analysis limits transparency and threatens the right to a fair trial. Algorithmic bias can reproduce existing social inequalities, increasing the risk of wrongful prosecutions. Additionally, the continuous alteration of digital evidence by AI systems weakens chain-of-custody standards, creates privacy risks, and may unfairly shift the burden of proof onto the accused.

India has taken important steps through the DPDP Act, the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Sakhshya Adhiniyam (BSA), and the Bharatiya Nagarik Suraksha Sanhita (BNSS). However, these laws remain largely technology-friendly rather than AI-specific. As a result, probabilistic outputs generated by AI systems are often treated as factual evidence, which weakens the adversarial justice process. Further, procedural safeguards under the BNSS do not adequately prevent excessive surveillance or the misuse of digital metadata, increasing the risk of abuse.

The proposed Deepfake Prevention and Criminalization Bill, 2023 attempts to address these gaps by explicitly criminalising non-consensual sexual deepfakes, deepfakes created to incite violence or disrupt official proceedings, and those used for fraud or identity theft. The Bill also proposes the creation of a National Deepfake Mitigation and Digital Authenticity Task Force. This body would track the spread of deepfakes, recommend penalties, advise on technological safeguards such as digital watermarking and blockchain-based verification, and suggest privacy-protective measures. Although the Bill has not yet been enacted, it marks an important move toward AI-specific regulation and is intended to work alongside existing cyber and technology laws.

In conclusion, India's legal and technological systems must develop together to effectively respond to autonomous AI-generated harms, ensure accountability, and protect constitutional rights. Strong legislation, effective oversight, and responsible use of AI are essential to protect personal liberty, dignity, and justice while maintaining public trust in digital systems. By strengthening preventive governance, institutionalising victim-focused remedies, and updating laws to reflect the unique challenges posed by AI, India can better address threats such as digital arrest scams, deepfakes, and AI-enabled crimes, and move toward a safer and more just digital future.

(The writer is Final Year, LL.B. student of Guru Nanak Dev University, Amritsar)