
RETHINKING CRIMINAL JUSTICE IN THE DIGITAL AGE

Jheel Nagori, Institute of Law, Nirma University

ABSTRACT

Relationship between technology and crime has undergone a transformation during the era of digitalization. In addition to being used for discussion and reporting of crime, social media has made it possible for a criminal milieu to exist, whereby crime can be planned, organized and facilitated. Information available through social media has impacted victim selection, encryption has impacted planning of crimes, artificial intelligence makes it difficult to prove the veracity of evidence, and algorithm-based platforms make it easier for dissemination of misinformation that can result in violence, defamation, and civil unrest, these changes show that technology is not just creating new crimes, but is also transforming existing ones. Nevertheless, criminal laws continue to be seen as dealing with the digital crimes in the context of old-age technology. The present paper is concerned with the discrepancy that exists between the constantly evolving nature of the digital world and the relatively unchanged nature of the criminal justice system of India. An attempt has been made to demonstrate that the realm of cybercrime has moved beyond being a limited specialization and the modern-day digital technology is connected with nearly all forms of crimes covered under the Indian Penal Code, including murder, organized crimes, sexual crimes, fraud, and public order offenses. Through an examination of statutes, judicial pronouncements, criminology, and investigations, the paper tries to demonstrate that the criminal justice reforms of the future for India should be based upon adaptability and capability building related to technology, digital forensics, platform responsibility, and rights protection.

Keywords: Criminal Law, Criminal Justice, Cybercrime, Digital Technology, Social Media.

INTRODUCTION

The coming into being of social media has radically changed the way in which people communicate, do business, voice their opinions and engage in civic life. Social media sites like Instagram, Facebook, WhatsApp, X (formerly Twitter), Telegram, Snapchat and YouTube have been integrated into human communication on a deep level where personal identities, human relations, transactions and political dialogue take place. India, with one of the largest internet users in the world, having more than 900 million internet users, has seen a radical digital transformation through affordable phones and mobile data. Even as these changes have brought about enormous benefits for society, they have also brought about an era where criminal activity has been transformed to such an extent that the law fails to grasp it fully. Traditionally, crime was viewed in terms of a physical act that took place in an identifiable geographic area. Criminals often depended on observation, knowledge of the people, or criminal circles within their immediate vicinity to find victims and commit crimes. The criminal justice process was also structured around the use of tangible evidence, eyewitnesses, geographic jurisdiction, and traditional investigation methods. However, the digitization of society has changed this notion completely. In today's world, many crimes begin with the use of online technology and then spill over into the physical world. Alternatively, some crimes remain purely online but still cause considerable psychological, economic, and reputational damage. Social media is one of the most important catalysts of this change. In contrast to previous communication technologies, social media promotes the constant sharing of personal information, interactive experience, geographical networking, and algorithmic dissemination of the information provided. People willingly share information concerning their routines, work life, family relations, travels, financial goals, social circles, and other aspects of their lives without being aware of the consequences of doing so in terms of the security of personal information. The large amount of freely available information changes the process of selecting a victim, as criminals can easily collect data, develop psychological acquaintance with victims and abuse their weaknesses without having any physical contact with them. As a result, social media becomes something more than just a communication tool; it becomes a place for various kinds of criminal activity.

The ability to create artificial voices, videos, images and digital persons has caused the complication of the existing principles of conducting the investigation and conducting court hearings. For hundreds of years, legal systems have operated under the presumption that

documentary and audiovisual evidence corresponds to reality until proven otherwise. However, the invention of advanced artificial intelligence has challenged the validity of this presumption through the ability to create fake evidence which can look no different than authentic one unless examined using special tools. Therefore, the courts will face the problem of electronic evidence authentication and reliability more often than before. Nevertheless, even with all these paradigm-shifting changes, legislative response tends to be reactive more often than anticipatory. The development of the criminal law follows a process that is quite sequential in its nature as it entails a discussion, analysis, interpretation, and adaptation of new legislation by different bodies, institutions, and courts. The advancement of technology, however, happens on a continuous basis as new platforms, new forms of communication, new applications of artificial intelligence and new forms of criminal activity appear in much greater volume than the development of legislation usually takes place.

It thus becomes clear that the problem facing the Indian criminal justice system goes beyond regulating cyber-crime. Digital technology has infiltrated such criminal acts as murder, extortion, kidnapping, organized crime, sexual assault, financial fraud, trafficking, terrorism and public order offenses. Social media no longer just records crimes committed or communicates after their commission, increasingly, social media plays a role in the conception, organization, commissioning, investigation, prosecution and perception of the crimes committed.

THE EVOLUTION OF CRIME IN AGE OF SOCIAL MEDIA

Crime has always been a dynamic concept throughout history. Criminals have developed their methods and modus operandi in response to changing societal structures, technological advances, shifts in economic systems and forms of human interaction. As societies developed from rural communities to industrial societies and finally to digitalized economies, crimes have developed in line with these transformations. Crime in the past was very much determined by geographical limitations. The offenders would usually target those individuals who were physically close to them because the geographical closeness was needed for surveillance and for communication. There would be a need to interact with the victim face-to-face, to write something to the victim or use criminal organizations nearby. Fingerprint, weapon, written document, testimonies of witnesses and other tangible objects would form the bulk of the evidence. Investigations therefore would require a great deal of intelligence from the local

police force, forensics examination of the physical evidence and testimony of the witnesses from the community.

The industrial revolution and urbanization have gradually brought about certain changes by creating dense population, transportation network and mobility. Crime syndicates began forming in the growing cities and new forms of economic crimes became possible due to economic progress. The emergence of the Internet at the end of the twentieth century was the first major revolution in this conception of crimes. The possibility of exchanging electronic messages enabled perpetrators to interact across geographical distances without having any physical interaction, and online banking and trading made possible committing financial fraud, identity theft, hacking, and unauthorized access to computer systems. However, the emergence of social media has completely changed the interaction of technology and crime. Unlike early Internet which was used only for exchanging information, social media encouraged people to provide personal information regarding their lives voluntarily. Individuals started sharing personal details about their everyday life, friends, travel plans, their achievements in terms of finances, places of study and work, political views, and family life using their public digital profiles. Additionally, the emergence of social media has made it impossible to distinguish between organized crime and usual criminal activity. A person who possesses smartphone, encrypted messengers, artificial intelligence services, and publicly accessible information can commit crimes that needed complicated criminal organizations before. Fraudsters can impersonate officials using AI-voice recordings, blackmailing people based on manipulated images, create fake investment platform in minutes, and talk with many potential victims using automatic messaging services.

Grooming, money laundering, identity theft, radicalization and stalking on the internet could be developed over several weeks or months before reaching their peak with a criminal offense. Therefore, victimization is a process rather than an individual event which makes it much harder to recognize early signs by victims and police agencies. Crimes have been expanding their focus towards reputation, emotional health, privacy, and autonomy in addition to physical security. Intimate image non-consensual sharing, cyber bullying, online harassment, deepfake pornography, and organized online defamation campaigns could leave a deep impact on the psyche of individuals without involving any physical contact. Technologies based on artificial intelligence allowed offenders to create synthetic voices which could trick the family members through financial frauds, create videos of events which have never taken place, automated

phishing attacks, fake identities and digitally manipulated evidence. These facts show that the current crimes can no longer be viewed as mere extension of traditional crimes to online space. Thus, the criminal justice system will need to cope not only with the creation of new crimes but also with reality where technology has been incorporated into crime committing process and investigation.

HOW DIGITAL PLATFORMS ARE RESHAPING CRIMINAL BEHAVIOUR

Besides the change that the growth of social media has brought about in the mode of communication, it has revolutionized the social environment where criminal behavior develops. Contrary to the case with traditional media, social media platforms do not depend on editorial boards and journalists whose job is to filter out any news item before publication. Algorithms have taken the place of editors and journalists on these platforms. The algorithms are used by the platforms to predict the content that will attract the attention of the users. They work in a manner such that they maximize user attention, increase viewing time, create interactions, and increase advertising revenue. However, while the system has made digital communication faster and more efficient, it has created some unintended effects. The problem is that the architectural design of these platforms tends to magnify the contents that the offenders can utilize for their criminal activities. In the present-day digital economy, human attention is one of the sources of wealth. As the information travels through several platforms, it becomes a mixture of facts, edited versions, disinformation, and manipulation of opinions.

The advent of digital trial by media whereby public opinion is formed independent of legal processes. the constitutional presumption that every accused individual is considered innocent until proven guilty has become increasingly difficult to maintain in the light of digital technologies facilitating instant judgments based on wrong information. Messages about nonexistent kidnappings of children, doctored videos meant to create religious conflicts, and baseless accusations against people have been spreading quickly on digital networks, leading to panic attacks and violence long before the authorities could step in. Albert Bandura's Social Learning Theory whereby individuals acquire certain behavior by observing, imitating, and reinforcing. Conventionally, people learned behavior from family members, peers, educational institutions, or the community. Social media has immensely increased the number of sources of influence by giving access to millions of people. The increased availability of artificial intelligence is bound to create issues about the authenticity of digital evidence. For many years, photographs, video footage, and audio recording have served as critical sources of evidence in

criminal and court procedures. Modern AI systems have greatly decreased these difficulties by making digital manipulation easily attainable by using commercially available software. The question for policymakers is not if there should be regulation of technology but how such regulation can promote innovation and democracy while limiting its use by criminals.

IS THE LAW KEEPING PACE WITH TECHNOLOGY

India has an extensive set of laws for crimes committed through the use of digital technology. The Information Technology Act, 2000¹ which was created to provide legal provisions for e-commerce and the use of electronic record keeping became the first Indian law which addressed cybercrime. While the Act has provision on hacking, unlawful access to computer systems, identity theft, data protection, and e-governance among others, it was developed during an era where social media sites, artificial intelligence, encryption apps and algorithmic digital ecosystem had not yet come into existence.

The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS),² Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS),³ and the Bharatiya Sakshya Adhiniyam, 2023 (BSA)⁴ can be seen as an effort to update the country's criminal justice system. The Bharatiya Nyaya Sanhita updates the Indian Penal Code which has colonial roots with provisions for contemporary criminal acts. On the other hand, the Bharatiya Nagarik Suraksha Sanhita contains changes that will enhance the processes of investigations and criminal trials. In addition, the Bharatiya Sakshya Adhiniyam which has replaced the Indian Evidence Act provides provisions on the inclusion of digital evidence within the criminal justice process.

Another one of the most critical legal problems is that related to the collection and storage of digital evidence. In contrast to traditional physical evidence, electronic data can change, delete, encrypt, or be transported internationally within seconds. Law enforcement agencies rely on data from mobile phones, cloud storage, records from social media, location data, surveillance recordings, financial transactions, and other electronic communications to piece together criminal activity. But in order for such evidence to be credible, there must not be a break in the chain of custody.

The issue of jurisdiction is yet another example of how technological developments have tested

¹ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

² Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

³ Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

⁴ Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).

established laws. The criminal law has long been based on the idea of jurisdiction, whereby a certain geographic location determines the jurisdiction of investigative authorities and courts in case of criminal acts. Digital crimes often violate these jurisdictional boundaries. Encryptions play a crucial role in ensuring privacy, confidentiality, financial dealings, and cyber security for the nation as a whole. On the other hand, the criminals use encryptions to conspire against the nation, distribute illegal information, engage in fraud, and hide information from the investigating agencies. This poses a challenging constitutional dilemma. Unconditional access by the government to encrypted information may infringe upon the basic right to privacy guaranteed by Article 21 of the Constitution⁵ after the judgment of Supreme Court in the case of “*Justice K.S. Puttaswamy v. Union of India*”.⁶ The creation of deepfake technology, voice cloning, synthetic media, and AI impersonations is a form of harm that does not always fall into conventional legal categories. In one case, a video created falsely showing the individual doing anything criminal or sexual might be extremely humiliating despite the fact that the incident never took place. However, there is a problem of defining the extent of platform liability as well because too much liability might result in censorship while less liability may provide platforms with opportunities to grow into places of misinformation, online harassment, fraud, hate speech, and conspiracies. The primary limitation of today’s legal responses, perhaps, is that these measures are inherently reactive. Criminal laws are created only when a particular form of behavior has already become prevalent within society. On the other hand, technology evolves constantly, thanks to its innovative nature. Even if legislators manage to detect certain emerging threats and work on the corresponding law, by the time the legislation is passed, technological ecosystems might have moved elsewhere. The balance between technology and criminal law cannot be viewed in terms of a struggle between innovation and regulation. Both must exist in the context of a constitutional order, which will ensure individual freedom, technological development, public security, and the rule of law.

WHY THE CRIMINAL JUSTICE SYSTEM FACES STRUGGLES IN CRIMINAL ERA

However, the efficiency of a criminal justice system is more than having punitive laws in place; it also requires an efficient investigation process, collection of legal evidence and judicial proceedings. In the case of India, some legislative changes such as Bharatiya Nyaya Sanhita have been witnessed as a result of the difficulties that are involved with dealing with crimes

⁵ INDIA CONST. art. 21.

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

committed using technology. Investigators face challenges in that the amount of digital evidence collected comes from different sources and therefore is difficult to filter. Digital evidence is fragile and thus subject to alteration and even destruction remotely, hence requiring stringent forensic practices in order to preserve its integrity. End to end encryption is another challenge that has come into play because while it helps to secure the communication, criminals have found ways of exploiting the same technology. The international nature of crimes also brings the challenge of cooperating with other nations in solving crimes, a task which proves to be difficult because of the various legal procedures. The use of private technology companies in providing crucial information is another challenge that comes with digital crime. Also, many investigative agencies lack well-trained personnel that affects conviction rates through poor handling of evidence.

AN ADAPTIVE AND TECHNOLOGY-RESPONSIVE LEGAL FRAMEWORK

The quick pace of technological advancement has completely altered the relationship between crime, society, and laws. Social media, artificial intelligence (AI), encrypted communications, and digital financial transactions have not only revolutionized the process of committing crimes but also changed the ways in which crimes are investigated and prosecuted. The legislative amendments of criminal justice systems cannot be the sole response to technological changes. In addition, criminal justice systems will always lag behind the criminals who constantly exploit the newly developed technology. The future of criminal justice needs to be about adaptability rather than the periodic reform of the legislative framework.

One way of doing this would be the use of technology-neutral principles in the criminal justice system instead of technology-specific laws. Laws aimed at specific software or platform become obsolete very soon due to the quick technological advancements. Instead, the focus of the criminal justice system should be on harmful behavior in order to ensure that offenses like fraud, extortion, identity theft, and forgery remain criminal irrespective of the technological platform employed.

Reform of legislation should be combined with organizational change as well. Law enforcement organizations need experts in digital forensics, cybersecurity, artificial intelligence, cryptocurrency investigations, blockchain analysis, and preservation of digital evidence. Contemporary investigation involves the analysis of digital data, tracing of online money transactions, authentication of electronic evidence, and identification of anonymous

individuals. In the same way, judges need to have adequate knowledge about technology to examine digital evidence and expert opinions. Enhancement of forensic laboratories, introduction of uniform rules of evidence preservation, and development of special forensic competences are no less necessary, especially in connection with undetectable audio, video, and images generated by artificial intelligence.

Effective functioning of criminal justice system presupposes cooperation of the government and digital platforms as well. Social media, cloud services, and instant messaging often have important data for criminal investigations while protecting the privacy of their users. The proper legal procedure, judicial oversight, and clear procedures of access to electronic evidence will help to balance the requirements of investigations with constitutional rights. As cybercrime often is committed beyond national borders, India needs to enhance international cooperation and cross-border evidence exchange mechanism.

On the other hand, criminal justice reform is not only about the implementation of constitutional principles. Technology cannot become an excuse for excessive surveillance or restriction of personal liberties or rights to freedom of speech. It is evident from the example of artificial intelligence, which may help with investigations due to the automation of the investigation process and digital forensics. However, its implementation may lead to mass surveillance and algorithmic discrimination. The development of criminal justice cannot be based on increased penalties and punishment but rather on the institution that will be able to adjust to technological progress and uphold constitutional values. India does not need to introduce any new criminal justice system; it needs an institution that will incorporate the knowledge in technology and science into the constitutional framework.

CONCLUSION

The digital revolution, on the other hand, presents a wholly different challenge because it not only brings about new techniques of criminality; it changes the whole context within which criminal activity takes place. Criminal activity now transcends geography, physical contact and old paradigms of investigation. There has been a move towards networking, data management and technological sophistication. The legitimacy of the law has always been defined by its effectiveness in responding to social changes without compromising on issues of justice, fairness and human dignity. The task before the law in this age is much more complicated but no less necessary.

It must be recognized that the evolution of crime is a challenge not only technological in nature but also a constitutional one. The aim must be to construct a criminal justice process which is technologically literate without being technologically dependent, pro-active without being invasive, and efficient without threatening the democratic freedoms upon which the constitutional framework is based. In doing so, the law will ensure its continued effectiveness in a world in which innovation changes not only the prospects for human advancement but also the ways in which criminal behavior develops.