E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 13-05-2023
Accepted: 29-06-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 1; 2023; Page No. 816-820

The role of technology in modernizing criminal law: Addressing cybercrime and digital evidence

Dr. Ajay Kumar Pandey

Assistant Professor, Department of Law, Sri Krishna University, Chhatarpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.14214746

Corresponding Author: Dr. Ajay Kumar Pandey

Abstract

The rapid advancement of technology has profoundly influenced criminal law, particularly in addressing the complexities of cybercrime and the use of digital evidence. Cybercrimes such as hacking, identity theft, phishing, and online harassment pose unique challenges due to their cross-border nature, the anonymity of perpetrators, and the dynamic evolution of digital platforms. This study explores the role of technology in modernizing criminal law to combat these crimes effectively. It examines the legal frameworks governing digital evidence, focusing on admissibility, authenticity, and chain of custody. Furthermore, the research highlights the challenges faced by law enforcement agencies in investigating and prosecuting cybercrimes, including jurisdictional issues, data encryption, and the misuse of emerging technologies such as artificial intelligence and the dark web. Emphasis is placed on the need for updated legislation, international cooperation, and advanced training for legal and law enforcement professionals. By integrating technological innovations and fostering global collaboration, criminal law can better adapt to the digital age, ensuring robust mechanisms to protect individuals and organizations from cyber threats. This paper underscores the importance of a proactive, technology-driven approach in modernizing criminal law to address the evolving landscape of cybercrime effectively.

Keywords: Advancement, cyber, threats, criminal, technologies, modernizing, jurisdictional

Introduction

Within the framework of this fast-developing digital era, the introduction of new technologies and innovations has left an everlasting mark on every aspect of life, including the police force. Many new and exciting possibilities for the judicial system's access to, analysis of, and processing of relevant data have arisen as a result of digital transformation. The rapid advancement of technology and invention has greatly impacted many areas of human endeavor, including the field of law. A key component of modern law enforcement is the use of technology. However, positive law, which refers to the rules and regulations that regulate the use of technology, is often behind the speed of technological growth. According to Lawrence Lessig's book Code and Other Laws of Cyberspace, the rules and laws that govern conduct in the digital realm are defined in large part by computer code. He stresses the significance of understanding how new technologies have altered the structure and functioning of the judicial system.

One such major player in the area who has contributed much to our knowledge of how technology and law are interdependent is Richard Susskind. Professor Susskind has brought attention to the profound effect that technology has had on both the theoretical and practical parts of law enforcement in his role as a preeminent legal scholar in the area of technology and law enforcement. Critical conversations on the future of law enforcement have been sparked by his ideas in "Online Courts" and "The End of Lawyers? The corporate environment has become more complicated, expensive, and hazardous due to the introduction of new technology. Organizations must adjust to survive the ever-evolving business landscape, intense competition, and lightning-fast technological advancements. Innovation in technology is both an essential resource and an integral part of the business. Therefore, technological advancements greatly impact the company's capacity to maintain competitiveness and attain sustainable profitability in the long run. Technology presents chances for firms to enhance their operations and services, as well as to support their business objectives in today's market. One may argue

that a company's or organization's ability to respond to and adapt to technological innovation determines its or her long-term success.

The rise of ICT in this turbulent age has altered the economic, social, and legal terrains in significant ways. Changes in many areas of human activity, such as communication, employment, and environmental relationships, have been accelerated by technological advancements. Despite the many benefits, the proliferation of fast-moving technological innovations like the internet, AI, automation, and cloud computing has given rise to a plethora of intricate legal concerns. People, businesses, and governments are all impacted by the new opportunities and challenges brought forth by technological advancements. The quick adaptation of the law to modern technological problems is one of the primary difficulties. Due to the exponential rate of technological change in the modern digital era, the law cannot depend on rules that have been in existence for decades. Particularly problematic from a legal standpoint are issues around cybercrime, data privacy and security, digital intellectual property, and sharing economy legislation. As a result, people are starting to pay greater attention to the moral questions raised by technology, especially when it comes to AI. The rights of individuals in relation to the use of personal data, the scope of digital surveillance, and the restrictions on free expression are all areas of heated controversy.

Cybercrime and electronic evidence: The globalization of threats

An estimated 14 trillion security events occur on networks annually, with millions of assaults reported daily against data and computer systems.15 Constant threats make it difficult to keep up with the news.16 Members of the Cloud Evidence Group have pointed out that cybercrime encompasses more than just assaults on computers. The rule of law, democratic societies, and individual rights are under grave danger from cybercrime, according to an analysis of the present size, extent, and difficulties associated with cybercrime and electronic evidence.

Hundreds of millions of people had their right to privacy violated due to the loss, misuse, or alteration of personally identifiable information (PII) that is processed and stored electronically. Some recent instances of massive data breaches include the following: the extortion and theft of 37 million Ashley Madison members' personal information, 15 million T-Mobile US users' information, and 150,000 TalkTalk UK customers' information. Forty million users' passwords and sexual preferences were reportedly for sale on the dark web in May 2016.

Therefore, cybercrime is an assault on people's dignity and integrity, especially children. There has been a fourfold increase in child abuse imagery over the past two years, according to the Internet Watch Foundation, an independent UK organization founded in 1996 by the UK internet industry. This is allegedly due to the fact that new technologies enable offenders to groom and procure children for abuse, and they are also 'fuelling a global boom in child sex tourism. Additional forms of cyberattacks that impact free speech include distributed denial of service (DDOS) attacks, website defacement, and others that attempt to undermine the accessibility of online resources. These attacks can target individuals, public institutions, civil society organizations, or media outlets. Thus, cybercrime is a major danger to our democracy and safety, regardless of whether it is committed by regular criminals or terrorists. On a daily basis, vital infrastructure, public organizations like parliaments and governments, and other institutions suffer assaults that need specialized knowledge and resources to assess the situation and limit any harm.

Areas where technology should be implemented

Though groundbreaking, the criminal justice system's use of IT still has a ways to go before it can be widely adopted and used to its full potential. Experts like April Pattavina have long argued that the criminal justice system as a whole needs to do more to use technology. There is a disparity in practicality because some individuals and organizations are great at adopting advanced technology, while others adhere to old ways. One way to address this is by implementing management and training programs that encourage stakeholders to embrace technology. Training in cultural diversity and gender sensitivity are examples of soft technology that may help the criminal justice system be better prepared to deal with new threats like terrorism and violence. Improving one's skills in areas such as intelligence gathering, information systems, and criminal investigation may also encourage expansion inside the system. Experts Alan Brown, Jerry Fishenden, and Mark Thompson all agree that the criminal justice system and government agencies must work together to successfully digitize. Cities like Mumbai, India, which are known for their multiculturalism, can potentially adopt this strategy after seeing success in the UK. The use of advanced technology such as DNA analysis, picture reconstruction tools, and artificial intelligence crime detection systems may streamline the judicial and law enforcement systems.

The significance of DNA testing in Indian law is shown by its legitimacy in instances like Nandlal Wasudeo Badwaik versus Lata Nandlal Badwaik.18 Promoting and stressing the significance of DNA technology, the government, the Law Commission, and legislative authorities are all working to get the word out. A commitment to using DNA and fingerprints for legal proceedings is shown by the establishment of organizations like the Centre for Cellular and Molecular Biology (CCMB).19 The use of IT in court hearings improves efficiency, streamlines procedures, and helps with time management.

Legal hearings can be more efficiently conducted, the backlog of cases may be reduced, and trial procedures can be made more efficient with the use of IT technology. To ensure seamless integration and maximize benefits, there must be well-structured systems and multi-layered approaches. Computer and IT advancements will continue to shape the future of law, with landmark statutes like the Indian Information Technologies Act serving as examples. Court processes and information processing may be enhanced via the use of current technology and the promotion of data interchange. Technology may introduce new complexities and transgressions, which necessitates ongoing adaptation and innovation; this much is acknowledged.

If the Indian court embraces system integration, promotes knowledge exchange, and cultivates an information culture,

it may make full use of information technology. Improving the system's efficiency and efficacy requires tackling challenges like time management and ensuring fast delivery of justice. If India's criminal justice system wants to evolve and gain the trust of its citizens, it must make use of modern technological tools.

Digital evidence

Any information or data that might be useful to an inquiry that is either saved on, received by, or sent by an electronic device is considered digital evidence. When electronic devices are confiscated and prepared for analysis, this evidence may be obtained. Information about people and events may be found in abundance in data that is collected online and/or taken from digital devices. Take game consoles as an example. These devices function similarly to personal computers and save a variety of data, including personal information, financial details, photographs, videos, and web surfing history.

When it comes to dealing with digital evidence, many agencies are falling behind. The fast evolution and widespread availability of digital gadgets, financial constraints, and an absence of suitable training opportunities are all factors that contribute to this. Due to the high expense of licensing, equipment, and manpower, digital forensics investigations are not always affordable. Securing buy-in from command staff requires proving a cost-effective return on investment. It may be especially difficult for smaller agencies to navigate the complex mix of federal, state, and local funds that might be used to fund these endeavors. Assuming law enforcement officials are aware of resources, regional models and other types of cooperation may be useful. While police academies do not currently include advanced digital evidence training in their mandatory curricula, officers at all levels of experience may come into touch with digital evidence sufficient to impact the case's result.

Information that is either kept or transferred in binary form and may be relied upon in court is known as digital evidence. You could find it on a mobile phone or a computer's hard disk. Common examples of e-crime that include digital proof include credit card fraud and child pornography. Information and data that is valuable to an inquiry and saved on, received from, or sent by an electronic device is known as digital evidence. (National Institute of Justice [NIJ], 2008).

Technology acquisition

According to Cyert and March (1963), organizations act rationally when they establish official objectives, develop strategies to achieve those goals, and finally use technology to support and assist those tactics. However, the fact that rationality has its limits is well known; objectives are not always clear, information on the optimal means of achieving them is sometimes lacking, and organizations have constraints due to people and material resources. Every business has its own unique setting, and the decisions it makes could be influenced by things beyond its control, according to the contingency approach. Organizations, according to the institutional viewpoint, have their own goals, such as maintaining existence, enhancing their reputation, making the most of available resources, and warding off dangers. Another view portrays organizations as chaotic rather than efficient machines, and it points out that organizations often come up with tactics and technologies to tackle problems before they even know there is a problem (Cohen, March, & Olsen, 1972). Because of this, organizational alternatives (such using technology) are often only sitting on the sidelines, ready to be used when the time is right.

Rogers (1962) proposed the diffusion of innovation model as a theoretical framework for understanding how businesses acquire technology. This model categorizes users of technology into five groups: innovators, early adopters, early majority, late majority, and laggards. While this taxonomy may have some intuitive appeal, the diffusion-of-innovation model has limitations when it comes to effectively describing how police agencies acquire technology. Even when thinking about just one kind of technology, police departments do not neatly fall into any one category. Aggregate mapping without incident-based geocoding might indicate that an organization is either ahead of the curve or falling behind in its use of GIS technology. Also, although one agency may be at the forefront of BWC innovation, another may be woefully behind the curve when it comes to LPR utilization. Therefore, a more thorough theoretical framework is required to characterize the procedure of acquiring technology in the police force, even if the diffusion of innovation model could serve as an effective foundation.

Further research is also required to identify the most important elements that agencies consider when deciding which technologies to purchase. There is evidence to suggest that departments do not always base their technology acquisition choices on what has been proven successful in attaining important police objectives, even if this would make sense. There is some evidence that law enforcement agencies choose, deploy, and integrate technology without considering the impact on departmental operations, strategic choices, or crime results. Essentially state that law enforcement agencies often use new technologies without fully considering the consequences. This description needs further investigation to see whether it is accurate and if it applies to all technical advances or just a subset of them.

Furthermore, there is still a lot of mystery about agency traits and how they may affect the acquisition of certain technologies. There is some data that suggests that the likelihood of an agency adopting certain forms of technology may be influenced by its size and location (e.g., Chamard, 2002, 2003, 2006), however the exact processes that explain this are not fully understood. Some think that larger organizations are more likely to have additional traits that make them more open to new technology. For example, it is reasonable to assume that bigger organizations have more money to spare for technology investments (Mastrofski, Parks, and Wilson, 2003). Because specialized units need certain technologies to perform their function at the highest level, it stands to reason that larger organizations may have a greater diversity of job functions, which is indicated by prior research as a higher degree of specialization within the larger organization. This, in turn, would lead to more adoption. Computerization and information technology (IT) skills have also been linked to

an increased proportion of technical workers. Consistent with previous results in innovation research, the notion that agencies with more specialized units are favorably linked to technical advances.

The transnational dimension of It investigations

The worldwide aspect of IT is one of the elements discussed before, especially when it comes to digital evidence. Space and national boundaries in this setting have an entirely different meaning than in the conventional physical universe. State attempts to build effective and rapid channels of collaboration were prompted, in particular, by the necessity to address crimes perpetrated using computer devices or the Internet, which in most instances have a global aspect. Consequently, international instruments pertaining to information technology investigations promote specific forms of collaboration, in addition to regional general mutual legal aid mechanisms and bilateral treaties.

When confronted with worldwide collaboration of investigative and judicial institutions, the defense naturally faces a number of challenges. Due to variations in national institutions and practical considerations, it is more difficult to contest evidence obtained in another country than evidence obtained inside one's own borders. Since digital information can traverse borders far more readily than physical things and people, it is more likely that some of the investigations will need to be carried out overseas.

Additionally, the potential for parallel procedures to be begun in various countries is enabled by criteria on jurisdictions that are supplied at the national level and supported by international regulations. This is true even in cases when investigative activities are conducted abroad at the request of a prosecuting authority. As a result of being subjected to different intrusive powers for the same alleged facts, the defendant runs the danger of violating the principle of ne bis in idem, which is a fundamental right recognized by most national systems and international human rights instruments. This could lead to punishment for the same offense twice. There are no binding and effective procedures to avoid or resolve instances of concurrent exercise of jurisdiction in various nations, either on a global or regional scale (like the EU system). Cybercrimes, in light of this legislative gap, seem to carry a greater danger of concurrent actions involving the same facts as more conventional forms of criminal wrongdoing.

The development of international collaboration has mostly been driven by the demands of the prosecution, rather than providing opportunities for the defense to exercise their rights or obtain pertinent information overseas. Actually, "an independent position to request international co-operation in any of the instruments of the Council of Europe or of the European Union" has not been bestowed upon the defense.

Defense priorities have been downplayed even at the regional level, despite the fact that there have been several attempts to enhance cooperation in criminal situations in recent decades. When we consider the European Union, we see that crucial measures to protect defense rights have been introduced in recent years. The new "constitutional" framework seems to seek a reasonable compromise between freedom and security, giving proper weight to the preservation of basic human rights, and the first legislative instruments devoted exclusively to defense rights have been approved. But when confronted with international inquiries, the defense still has a poor position, as noted in the literature. For a number of reasons, including the fact that the EU legislator has only dealt with a subset of defense rights, leaving the remainder to be governed by national laws, and the fact that different countries still take very different approaches to a subset of defense rights, meaning that issues related to the fragmented setting persist. It is also believed that the defense would have a harder time challenging evidence obtained overseas as a result of the change from mutual legal aid to mutual recognition.

When looking at digital investigations from a defensive perspective, the most concerning issue is the danger that some investigative methods offer to the idea of territoriality. In light of the opportunities presented by IT for the global storage and remote access to personal data, borders seem to dissolve. It is possible that investigators are unaware of the precise location of data; nevertheless, by using cloud service providers, they may have access to data that is fragmented and spread across many countries. Additionally, by using certain software, they may even get online access to data stored on a computer in a different nation. Different standards of protection of basic rights are the primary worry of an individual residing in country A who is exposed to investigative invasive powers from country B. Similar to how foreign law enforcement agencies are typically not allowed to conduct searches within their own borders, a "virtual" invasion into one's private sphere by foreign authorities utilizing their own domestic standards would naturally give rise to valid concerns; this is one facet of national sovereignty. Klip notes in Section 4 of the General Report that individuals may have a reasonable expectation of security even in the 'anarchic' cyber environment, and that the state ostensibly responsible for providing security "can only be the state that has the power and the obligation to protect."

By connecting them with the national law of the subject's location and mandating and limiting extra-territorial interception without MLA, this EU instrument appears to address both sovereignty concerns and the threatened freedoms of individuals subject to transnational interceptions. However, not every EU member state has signed this document, and some national courts have a tendency to accept the findings of interceptions made without MLA without much debate. Consequently, it is very uncommon for foreign investigators in other countries to intercept a person's communications without asking for mutual help or disclosing the nation in where the individual is situated.

New trend in cases of forgery and fraud-a detail study

Some of the most prominent developments in the last few decades including cybersecurity, AI, blockchain, cloud computing, and the IOT (internet of things) have emerged in response to the COVID-19 pandemic. All the way from the countryside to the city, these technologies have made their way into the economy. The proliferation of new technologies has made it easier for thieves to commit crimes by providing them with additional entry points into digital systems like ATMs. Once the hackers have access to the ATM's operating system, they may manipulate it to print

money. Maintaining law and order for the safety and peace of society and developing a sense of logical understanding in all aspects of technological developments as users are essential requirements for all intellectual investigating officers, court officers, judicial officers, and those involved in making laws as a deterrent. These broad insights may greatly aid in making laws more accessible to the public and ensuring that they are accurate, consistent, and up-to-date. The criminal justice system may potentially benefit from this as well, particularly when it comes to presenting forensic evidence in court using credible data. Agencies throughout the world are now better able to handle data, share information, and communicate thanks to new devices and equipment that link to computers and cellular technology. The criminal justice system's ability to administer fair punishment must improve as a result of this. The development of technologies to better investigate crimes online has been driven by the growing social reliance on the Internet/cyber domain and computer-mediated interactions. Every one of us has to stay up-to-date on the newest cutting-edge innovation before we can use it to comprehend how criminal activities have evolved in relation to the digital influence on the criminal justice system. To solve modern criminal cases, forensic scientists must refresh their knowledge of technology developments. This is an essential requirement of the moment.

Conclusion

The need for constant internet connectivity has grown in modern society, but law enforcement has taken measures to discourage people from engaging in cybercrime, including passing new laws and policies, ensuring their implementation, and raising user awareness and education about the risks associated with new technologies. The utilization of new investigative techniques, simplified access to information, and streamlined legal procedures are all made possible by technological improvements. But we also need to solve problems with access inequity, privacy, and ethics. Therefore, it is important to work toward a future where technological advancements serve to strengthen, rather than weaken, the fundamental concepts of justice inside our legal system. There may be good or bad results to the new research on how innovation and technology affect justice in the police force.

References

1. Hasibuan EJ, Pulungan W, Siregar M, Muda I. Tourism communication in development Sipirok City, South Tapanuli Regency. International Journal of International Relations, Media and Mass Communication Studies. 2021;7(2):33-45.
2. Kadir A, Tarigan U. Peranan Dinas Tata Kota dan Pertamanan dalam Upaya Peningkatan Pelayanan Izin Mendirikan Bangunan (IMB) di Kota Tanjungbalai. c2018.
3. Koloay R. Perkembangan hukum Indonesia berkenaan dengan teknologi informasi dan komunikasi. Jurnal Hukum Unsrat. 2016;22(5):16-27.
4. Lucas M. The impact of technology on the criminal justice system. Danial Khan Department of Public Health, Yale University; c2023.
5. Muda I, Hasibuan EJ, Pulungan W, Siregar M. Tourism potential of Percut village, Percut Sei Tuan District, Deli Serdang Regency. International Journal of Progressive Sciences and Technologies. 2022;30(2):160-165. DOI: 10.52155/ijpsat.v30.2.3927.
6. Muda I, Hasibuan EJ, Siregar M, Pulungan W. Harmonization village based on Dalihan Na Tolu in Sibadoar Village, Sipirok District, Selatan Tapanuli Regency, Indonesia. Path of Science. 2022;8(10):4001-4007. DOI: 10.22178/pos.86-4.
7. Natamiharja R, Putri RW, Banjarani DR, Setiawan I. Perlindungan keamanan digital di era Society 5.0 dan implementasinya di Indonesia. 2022;61.
8. Putri MC, Sinaga EMC. Disrupsi digital dalam proses penegakan hukum pada masa pandemi COVID-19. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional. 2021;10(1):79. DOI: 10.33331/rechtsvinding.v10i1.625.
9. Santoso MH, Hutabarat KI, Wuri DE, Lubis JH. Smart industry inkubator otomatis produk pengering ikan asin berbasis Arduino. Jurnal Mahajana Informasi. 2020;5(2):45-53.
10. Santoso MH. Application of association rule method using Apriori algorithm to find sales patterns: Case study of Indomaret Tanjung Anom. Brilliance: Research of Artificial Intelligence. 2021;1(2):54-66. DOI: 10.47709/brilliance.v1i2.1228.