

WHEN CRIME GOES DIGITAL: FORGING JUSTICE IN AN ERA OF INVISIBLE THREATS

-Abdul Ashik Mubarak Rawoother¹

"You can't defend. You can't prevent.

The only thing you can do is detect and respond."

— Bruce Schneier

Abstract

Rapid societal digitization has changed how people, groups, and governments communicate, bringing with it both previously unheard-of opportunities and risks. The extent and complexity of cybercrime are growing along with information and communication technologies (ICTs). Cybercrime is a serious threat to national security, economic stability, and individual privacy. It can take many forms, from identity theft, financial fraud, and cyber stalking to massive data breaches and cyber terrorism. Simultaneously, the idea of digital justice has become a crucial framework to guarantee that social, ethical, and legal standards change to meet the demands of the digital era. The article investigates the intricate and dynamic field of cybercrime and how it relates to digital justice. It critically assesses current legal systems and their ability to successfully combat crimes made possible by technology while defending basic human rights in the online sphere. The study draws attention to the shortcomings in international collaboration, regulation, and enforcement, especially in countries with weak cyber laws. It also explores how blockchain, artificial intelligence, and digital forensics might be used to identify and prosecute cybercrimes, highlighting the necessity of technological adaptability in the judicial system. Furthermore, the study examines digital justice as a proactive approach to guarantee due process online, encourage fair access to digital technologies, and shield underprivileged communities from online harms, rather than only as a response to cybercrime. As essential elements of digital justice, concerns about algorithmic unfairness, data ownership, and monitoring are examined. The study takes a multidisciplinary approach, combining knowledge from computer science, ethics, criminology, and law to suggest a framework for a more robust and equitable digital ecosystem. Ultimately, this research underscores the need for an inclusive and adaptive digital justice system capable of addressing the multifaceted challenges of

¹ Associate Professor, Al Ameen College of Law, Bangalore.

cyber-crime in a globalized and interconnected world.

Keywords: *Cyber-crime, Digital justice, Cyber security law, Technological forensics, Data ethics*

Introduction

In today's digitally interconnected world, cybercrime has emerged as one of the most significant threats to individuals, organizations, and governments globally.² Cybercrime refers to criminal activities that are committed using computers, networks, or digital devices, often targeting information systems, data, or online users.³ These crimes range from identity theft, hacking, and financial fraud to more complex offenses like ransomware attacks, cyber espionage, and cyber terrorism.⁴ The anonymity and borderless nature of the internet make cybercriminals particularly difficult to track and prosecute, creating unique challenges for law enforcement and legal systems worldwide.⁵ As technology continues to evolve rapidly, so does the sophistication and variety of cybercrimes, demanding equally adaptive and robust responses to ensure digital security, privacy, and justice.⁶ The technological inundations had already started perforating the legal by the middle of the 20th century. The evolution of computers had taken the path of sophistication and technical excellence, and with it, the face and form of crime was becoming more automated, more advance.

Definition and conceptualization of cyber crimes

Computers do not commit crimes.⁷ However, the computer hand in hand with the Internet has given birth to a new generation of crimes. In such computer crimes, the role of human hand is less while the major activities are carried out by the automated machines. While the Internet is the wonder gift of science to mankind, it has at the same time become a haven for criminals⁸

² Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

³ Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

⁴ McQuade, S. C. (2012). *Understanding and Managing Cybercrime*. Pearson.

⁵ Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.

⁶ Brenner, S. W. (2010). *Cybercrime and Digital Justice: Responding to the New Threats*. Routledge.

⁷ Donn B. Parker, a retired guru, however, anticipates a day of "Automated Crime" when a software package will be available which when put to use will automatically select the victim, anonymously commit the crime and remove the evidence of its commission from the computer. Donn B. Parker, Automated Crime" in Cyber-crime [International Conference Course Book] (Oceana Publications, Washington DC 1997)

⁸ 1. Web crime statistics: Total complaints filed in 1993 (1-7 per day), it went up from a total of 971 (2.6 per day) in 1994 to 1494 in 1995, to 4322 in 1996, to 12,775 in 1997, to 47,000 in 1998 and to almost 1,00,000 in 1999. It was projected to be more than 2,80,000 in the year 2000 at a phenomenal rate of almost 775 complaints per day. Most common reports/complaints are of: Child pornography Fraud 35 per cent 33 per cent

Definition of Cyber Crimes⁹

The words "cyber-crimes" and "computer crimes" are used interchangeably in common parlance. The word "computer crimes" has wider ambit as it entails not only crimes committed on the Internet but also offences committed in relation to or with the help of computers.¹⁰ Donn B. Parker¹¹ distinguishes between the concepts of computer crime and cyber-crime, and gives the definitions of the terms in the following words:

- I. Computer crime A crime in which the perpetrator uses special knowledge about computer technology.
- II. Cyber-crime A crime in which the perpetrator uses special knowledge of cyberspace.

A computer crime is defined by the US Department of Justice ¹²as an illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution". But the definition is not exhaustive as there are many acts which can be called abusive activities concerning the computer but "they are often not clearly illegal"¹³ Moreover, most of the cyber-crimes are committed via the Internet but the definition has no reference to it. Cyber-crimes can be plainly defined as "crimes directed at a computer or a computer system"¹⁴ but the complex nature of cyber-crimes cannot be sufficiently expressed in such simple and limited terms. There are many multilateral organizations recently involved in shaping high-tech crime policy.¹⁵ The Organization for Economic Co-operation and Development (OECD) has adopted the following definition as the working definition for computer-related crime or computer crime:

Computer abuse is considered as any illegal, unethical data" This or unauthorized behaviors relating to the automatic processing and transmission of data.¹⁶ This definition is also deficient as it refers only to the "transmission data" while cybercrimes are committed also through

⁹ Ferrera, Lichtenstein, Reder, August and Schiano, *Cyberlaw: Text and Cases* (West Thomson Learning, 2001) 297.

¹⁰ K. Verma & Raman Mittal (Eds.), *Legal Dimensions of Cyberspace* (Indian Law Institute, New Delhi 2004) 228

¹¹ A computer crime expert and a security veteran with 30 years of related experience. Steven Furnell, *Cyber-crime: Vandalizing the Information Society* (Addison-Wesley, 2002)

¹² Koba Associates, *Computer Crime: Expert Witness Manual* (US Department of Justice, Bureau of Justice Statistics, Washington DC 1980).

¹³ A report prepared by McConnell International, "Cyber Crime... And Punishment?" December 2000, <<https://www.library.cornell.edu/colldev/mideastcyerime.pdf>> last accessed 7-10-2015.

¹⁴ Peter Stephenson, *Investigating Computer-Related Crime* (CRC Press, Washington DC, 2000)

¹⁵ These are: European Union (EU), Council of Europe (CoE) and G8. Certain other organisations like the Organisation for Economic Co-operation and Development (OECD), United Nations (UN), Interpol and Europol are also involved to a lesser extent. Richard A. Wright & J. Mitchell Miller (Eds.), *Encyclopedia of Criminology, VolI (A-G) 1.1* (Routledge, New York, 200) 2

¹⁶ Suresh T. Vishwanathan, "The Criminal Aspect in Cyber Law" in *The Indian Cyber Law* (Bharat Law House (P) Ltd., 2002) 81.

transmission is defined as certain malicious programs and viruses. Some authorities also use the term "information technology offences"¹⁷ instead of cyber-crimes. Thus, Information technology offences have been taken to encompass any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer system.¹⁸

Doctrine of *mens rea* in cyber crimes

Mens rea has come to be recognized as an essential element of crime except in statutory offences where liability is strict. With the advent of e-crimes, the legal world faces the difficulty, besides many others to pin point mens rea in cyber-crimes. In cyber-crimes, one should see what state of mind of a hacker was and that the hacker knew that the access was unauthorized. Thus, a "particular computer" need not be intended by a hacker, it is enough if the unauthorized access was to "any computer". Thus, following two ingredients form the mens rea applied to a hacker¹⁹ The access intended to be secured must have been unauthorized. There should be awareness on the part of the hacker regarding the access. Awareness on the part of the hacker becomes easier to prove where he is an outsider and has no authority to access. But where a hacker already has limited authority as in the case of the employee of a company, it becomes difficult to establish that he exceeded his limits and was even aware of the fact that he is exceeding it.

Modus operandi of cyber crimes

Subject-matter of crime and more importantly its modus operandi. The entire criminal act consists of automated. The Internet has changed the machines and the human hand is only at the starting or ending points. This makes the challenge formidable. The challenges posed before the reasons: criminal system is mainly due to the following

1. The transnational nature of cyber-crimes where geographical limit and international boundaries have lost their meaning and a single criminal act passes through a number of jurisdictions.
2. The ever-expanding nature of the Internet and the backwardness of the present criminal law has rendered law, helpless and unresponsive.

¹⁷ The IT Act, 2000 (21 of 2000) has also used the term. The Act not only amends the IPC to bring within its scope conventional offences committed electronically, but also creates a new breed of information technology offences, the prevention of which are incidental to the maintenance of a secure electronic environment. These offences are found in Chap XI of the Act. Nandan Kamath, Chap 14 in Guide to Information Technology Act, Kues o Regulations (2nd Edn., Universal Law Publishing, 2001) 85.

¹⁸ Council of Europe, Recommendation No. R (9s) 13 concerning problems of criminal procedural law connected with information technology adopted by the committee of Ministers on 11-9-1995

¹⁹ Ankit Majumdar, A Practical Perspective on Hyper Linking, Framing and Meta Tagging" in Nandan Kamath (Ed.), Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing Co., 2002) 272.

3. The technicality involved in cyber-crimes makes investigation a highly complicated and purely technical job.

4 In detecting in detecting cyber-crimes throws biggest challenge to the legal system which is mainly based on evidence of some sort.

Cyber-crimes are crimes of the digital age. They are bloodless, non-violent uses of e crimes which are committed by computer literate persons whose way and method of committing the crime is highly sophisticated and technical. Most of the cyber-crimes are committed by a good number of accomplices called "outsiders and insiders" who are workers of communication and Internet service companies. Modus operandi is a system of actions of the criminal (and/or related persons) united by one intention directed on preparing, committing and covering up a crime, determined by objective or subjective factors and connected to use of corresponding facilities and means. Modus operandi of committing cyber-crimes mainly involves illegal interference in computer, computer system and network operation. Such illegal interference can be divided into various groups.²⁰

Indian Scenario

The Internet has a global face. India, too, being a formidable part of the globe, felt a seismic shift in the technological set-up when the Information Technology (IT) waves surged ahead and necessitated the formation of the IT ministry in the country in the year 1999. India was catching up with legal response to online activities and infractions when it came up with its first cyber legislation, namely, the IT Act, 2000. The Act has been amended in 2008, enforced in 2009 and has responded well to the men ace of cyber-crime in the country.²¹ To protect the Critical Information Infrastructure (CI), a new agency, namely, the Indian Computer Emergency Response Team (ICERT) is to be formed to respond to computer incidents in the country.²² Earlier in the year 2003, CERT was formed to issue instructions in the context of blocking websites.²³

Criminal liability of invisible players online

The Internet content flows though apparently between the user and the host yet no transaction is ended between the two parties exclusively. "Every Internet transaction requires the participation of multiple intermediaries, and may well involve more than two actors."²⁴ The

²⁰ Source: Vladimir Golubev, "Computer Crime Typology", Computer Crime Research Centre, 16-1-2004.

²¹ See chapter 12 of cyber crimes

²² Section 70 A and section 70 B inserted by the IT Amendment Act 2008

²³ Noticing the increase in the number of cyber-crimes in India, the Government of India issued notification by virtue of Ss. 67 and 88 of the IT Act to constitute a computer

²⁴ Chris Reed, Chap 2, "From Each According to His Ability: Actors and Activities in the Internet World" in internet Law: Text and Materials (Cambridge University Press,

fact is true not only in e-commerce transactions but in the entire crime line where the "principal actors"²⁵ have something to contribute towards the crime although their liability may not arise in each case. The position of the online intermediaries can be well understood by making a reference to the communication transmitters and landline carriers of yesteryears. The postal carriers and telephone network are the predecessors of these online intermediaries though the automated transmission marks the dividing line between the two.

Liability of ISPs

Who is an ISP? -ISPs are the mediators, the carriers of information and are the online counterparts of telecommunication companies. In addition to serving individuals, ISPs also serve large companies pro Points (NAPs). Providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access At the dawn of the Internet, the above answer was sufficient to describe an ISP but with the development of "Internet hardware and software gent in their roles, technologies"²⁶ the ISPs took multifaceted form and became more divergent in their roles. By contrast, Internet content providers who only provide information applications or convey. content is accessed by end-users but who do not provide access or services are not under legal obligation to own a licence.²⁷ As disseminated in a borderless world; basically the contours of liability of these online intermediaries including the ISPs are in connection with the content which is transmitted, copied or possessed by them which often offend the rights of individuals which either arise out of contractual | bond or are simply some sort of tort or criminal offence like defamation, copyright infringement, child pornography, false advertise a fraudulent misrepresentation, breach of confidentiality and privacy, and so on.

Types of Cybercrime

- **Identity Theft and Fraud:** Cybercriminals often use the internet to steal personal information, such as Social Security numbers, credit card details, or login credentials. This data is then used for fraudulent purposes, such as making unauthorized transactions or committing identity fraud.²⁸
- **Hacking and Unauthorized Access:** Hacking involves gaining unauthorized access to computer systems or networks, often with the intent to steal, modify, or destroy sensitive data.

²⁵ *ibid*

²⁶ Chris Reed, *Computer Law* (Oxford University Press, 2003)

²⁷ Graham J.H. Smith & Bird & Bird. *Internet Law and Regulation* (4th Edn., Sweet & Maxwell, London 2007)

²⁸ Anderson, R., et al. (2019). *The Economics of Information Security and Privacy*. Springer.

This type of cybercrime can range from small-scale intrusions to large-scale breaches, such as the hacking of government or corporate systems²⁹

- **Phishing and Social Engineering:** Phishing involves tricking individuals into revealing confidential information, such as passwords or financial details, by impersonating a trustworthy entity. Social engineering is a broader concept that involves manipulating individuals into breaking security protocols or revealing sensitive data.³⁰
- **Ransomware Attacks:** In ransomware attacks, cybercriminals infect a victim's system with malicious software that encrypts data, making it inaccessible. The attacker then demands a ransom from the victim in exchange for the decryption key.³¹ This type of crime has seen a dramatic increase, affecting individuals, businesses, and government institutions worldwide.
- **Cyberterrorism:** Cyberterrorism refers to the use of digital tools to cause fear, disruption, or harm, often with political or ideological motives. Cyberterrorists may target critical infrastructure, such as power grids, water supplies, or transportation networks, to create chaos³²
- **Child Exploitation and Cyberbullying:** Cybercrime also includes offenses that involve the exploitation or abuse of children online, such as distributing child pornography or engaging in online grooming. Cyberbullying, where individuals harass or intimidate others via digital platforms, has become an alarming issue, particularly among minors.³³

The concept of Digital Justice

Digital justice refers to the application of legal principles and ethical considerations to the digital world, particularly in relation to cybercrime. It involves the balance between protecting individual rights and ensuring that offenders are held accountable for their actions. Key areas of digital justice include:

Legal Frameworks for Cybercrime

As cybercrime often transcends national borders, digital justice must include the development of international legal frameworks. Treaties like the Budapest Convention on Cybercrime (2001) aim to harmonize laws across jurisdictions to combat cybercrime effectively.³⁴ However, challenges remain in enforcing these laws, as different countries have different legal

²⁹ Holt, T. J., & Bossler, A. M. (2016). *Cybercrime: The Insider's View*. SAGE Publications.

³⁰ Whitty, M. T. (2013). *Cybercrime and Society*. SAGE Publications.

³¹ Symantec Corporation. (2019). *Internet Security Threat Report 2019*. Symantec.

³² Denning, D. E. (2000). *Cyberterrorism: The Newest Threat to National Security*. Testimony before the U.S. Senate Subcommittee on Technology, Terrorism, and Government Information.

³³ Li, Q., & Yip, K. (2013). *Cyberbullying in the Digital Age: The Psychological Impact on Victims*. *CyberPsychology & Behavior*.

³⁴ Council of Europe (2001). *Convention on Cybercrime (Budapest Convention)*. Council of Europe.

standards and capabilities in addressing cybercrime.

Privacy and Data Protection

Digital justice involves ensuring that individuals' privacy and data rights are protected in the digital realm. Laws such as the General Data Protection Regulation (GDPR) in the European Union provide stringent measures to safeguard user data and offer victims avenues for redress when their data is misused.³⁵

Access to Digital Justice

One of the challenges in digital justice is ensuring equal access to legal remedies for all individuals, especially marginalized groups. With many people lacking knowledge of digital rights, there is a growing need for education and advocacy to help individuals understand and assert their rights in the digital space.³⁶

Cybersecurity and Prevention

Another aspect of digital justice is the proactive measures taken by governments, organizations, and individuals to prevent cybercrime. This includes public policy initiatives, cybersecurity programs, and creating awareness about best practices to protect digital assets.³⁷

Ethical Challenges and the Role of AI

With the increasing use of artificial intelligence (AI) in both criminal activities and law enforcement, digital justice must also address the ethical implications of AI. Issues such as algorithmic bias, surveillance, and the potential for wrongful convictions due to automated systems are important considerations in the field of digital justice.

Conclusion

The rise of cybercrime presents an unprecedented challenge to individuals, organizations, and governments worldwide. As technology continues to evolve, so too does the complexity and scope of cybercriminal activities, from identity theft and hacking to cyberterrorism and ransomware attacks. These crimes have far-reaching implications for personal privacy, economic stability, and national security, making it crucial to establish robust legal and ethical frameworks to protect individuals in the digital age. Digital justice plays an essential role in addressing the growing menace of cybercrime. The development of international legal frameworks, such as the Budapest Convention, has been instrumental in fostering cross-border cooperation among law enforcement agencies. However, much remains to be done to bridge

³⁵ European Union (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

³⁶ Susskind, R. (2019). *Tomorrow's Lawyers: An Introduction to Your Future*. Oxford University Press.

³⁷ Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731

the gap between technological advancements and legal capabilities. For digital justice to be effective, governments must prioritize stronger cybercrime laws, improve enforcement mechanisms, and ensure that digital rights, particularly privacy and data protection, are adequately safeguarded. Furthermore, the ethical challenges posed by emerging technologies like artificial intelligence and blockchain demand careful scrutiny to prevent abuse and maintain fairness in the justice system.³⁸

In conclusion, the fight against cybercrime and the pursuit of digital justice must be a shared responsibility between governments, the private sector, and individual users. Only through international cooperation, comprehensive legal reform, and continued technological innovation can we hope to create a safer, fairer digital world. As the digital landscape evolves, so must our efforts to protect the principles of justice in an increasingly connected world³⁹

³⁸ Brenner, S. W. (2010). *Cybercrime and Digital Justice: Responding to the New Threats*. Routledge.

³⁹ Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.