INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CHALLENGES IN INVESTIGATION AND PROSECUTION OF CYBERCRIME IN INDIA: A FORENSIC AND LEGAL ANALYSIS

AUTHOR – HARSHVARDHAN PRATAP SINGH* & DR. ANUPRIYA YADAV**

* STUDENT AT AMITY UNIVERSITY LUCKNOW

** PROFESSOR AT AMITY UNIVERSITY LUCKNOW

BEST CITATION – HARSHVARDHAN PRATAP SINGH & DR. ANUPRIYA YADAV, CHALLENGES IN INVESTIGATION AND PROSECUTION OF CYBERCRIME IN INDIA: A FORENSIC AND LEGAL ANALYSIS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (5) OF 2026, PG. 701-711, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The way digital technologies are growing in India is changing how people live their lives. This is affecting how people talk to each other how they buy and sell things how they learn and how they think about keeping their personal information private.. With all these changes there is also a big increase in cybercrime. What used to seem like cases of hacking or online scams has now become a big and complicated problem that affects not just individuals but also the whole system of justice. The police and other law enforcement agencies are trying their best. They are having a hard time keeping up with how fast and clever these crimes are.India has laws to deal with this like the Information Technology Act from 2000 and other laws related to crime. However when these laws are put to the test in life some problems become clear. Investigations into cybercrimes are often slowed down because the police do not have the technical skills they do not have the right equipment to analyze evidence and sometimes they are just not sure what to do. The evidence from devices, which is very important in these cases can be easily changed or damaged and it is not always handled in the right way. This makes it hard to prosecute the cases because even a small mistake can make a strong case weak.Another problem that people often do not think is important enough is that cybercrimes can happen from anywhere in the world. This makes it hard for the police in countries to work together. When you add to this the fact that people can use tools to hide their identities and that technology is always changing it becomes a very difficult task. It is like trying to catch something that is always changing shape.

This paper is trying to look at these problems in detail not from a legal point of view but also from a technical point of view. It is looking at how digital forensics can help with investigations while also being realistic about the problems that exist. At the time it is thinking about the need for changes in the law in the institutions and in the technology. Because in the end dealing with cybercrime is not about making stricter laws it is about creating systems that are flexible informed and ready, for what is coming next. Cybercrime is a problem and digital technologies are a big part of it so we need to think about how to deal with cybercrime using digital technologies. The laws and the systems we have now are not enough to deal with cybercrime so we need to make some changes to be able to fight cybercrime.

Crucial words: *Cybercrime, Digital Evidence, Cyber Forensics, Investigation, Prosecution, IT Act, Criminal Justice System*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Introduction

The way India has changed with the internet is really surprising. A few years ago nobody thought it would happen so fast. Now people do everything online from banking and learning to shopping and talking to friends with a few clicks. The internet is cheap most people have smartphones. The government is helping everyone get online. This has made India one of the growing internet countries in the world.. With big changes come big problems. Along with the things like being able to do things easily and stay connected there is a lot more cybercrime.. It is not getting better.[1]What makes this problem hard to solve is that cybercrime is different from crimes. Before crimes happened in one place. You knew who was there and what happened.. Cybercrimes like hacking, stealing identities, online fraud stalking on the internet and breaking into computer systems happen in a secret world. Someone can sit in one part of the world. Hurt someone on the other side of the world without leaving any clues. It is scary how easy it is.The internet itself makes things even harder. It has no borders it is always. People can be anonymous. Bad people can hide behind names, secret networks or masks that make it hard to find them. This means that the old ways of solving crimes like asking questions looking at evidence and talking to witnesses do not work well. The police need to adapt but it takes time, training and money which they do not always have.[2]From a point of view it is also very hard. The laws in India were not made to deal with these internet crimes. Even though there have been some changes there is still a gap between what the law says and what happens in real life. Investigators have trouble with the parts prosecutors have trouble presenting evidence and courts have to deal with new and unfamiliar issues.[3]

This paper tries to make sense of all this. It looks at the problems of solving and prosecuting cybercrime cases in India not from a legal point of view but also from a scientific point of view. Because digital science has become a part of solving cybercrimes. At the time this paper tries to suggest practical solutions, rather than just pointing out problems. It does not try to find a solution because there is not one but it tries to show ways to make the system better more prepared and more effective in dealing with cybercrime today. Cybercrime is a problem and this paper tries to help find ways to solve it by looking at the challenges of cybercrime and suggesting reforms that can help. The idea is to make the system more responsive, to cybercrime and to help the people who are working to stop it by providing them with the tools and resources they need to fight cybercrime.

Legal Framework Governing Cybercrime in India

When it comes to dealing with cybercrime in India, the legal framework is a mix of specialized legislation and traditional criminal laws adapted to modern contexts. On paper, it appears reasonably comprehensive. But once you start looking closer, especially from the perspective of investigation and prosecution, certain gaps and inconsistencies begin to show. It's not that the law is absent—it's more that it sometimes struggles to keep up with the speed at which technology evolves.[4]

2.1 Information Technology Act, 2000

The backbone of India's cyber law regime is the Information Technology Act, 2000. Enacted at a time when the internet was still in its early stages in India, the Act was a significant step forward. It gave legal recognition to electronic records and digital signatures, which was essential for the growth of e-commerce and online governance. But beyond that, it also laid down provisions to deal with cyber offences—something that was, at the time, quite forward-looking.[5]Over the years, the Act has been amended to address emerging forms of cybercrime. It criminalizes activities like unauthorized access to computer systems, hacking, identity theft, and cheating by impersonation in online spaces. These provisions, at least in theory, cover a wide range of cyber offences that are commonly reported

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

today. However, there is a subtle issue here… the law often uses terminology that can feel slightly outdated or too broad when applied to modern technologies like artificial intelligence, blockchain, or even sophisticated phishing techniques.

Another challenge lies in enforcement. Having provisions on paper is one thing, but applying them effectively requires a clear understanding of both legal principles and technical processes. Many cases falter not because the law is insufficient, but because its application becomes complicated in real-world scenarios. There are also concerns about overlaps between different sections, which can sometimes create confusion during investigation or prosecution.

2.2 Indian Penal Law

Interestingly, not all cybercrimes are dealt with under the Information Technology Act alone. A significant number of cases are prosecuted using provisions from traditional criminal law. Offences like cheating, fraud, criminal intimidation, forgery, and defamation—these are all covered under general penal laws, and they often intersect with cyber activities.[6]This dual framework can be both helpful and problematic. On one hand, it allows flexibility. Investigators can choose provisions that best fit the facts of a case, especially when the cyber element is just one part of a larger offence. On the other hand, it can lead to overlaps and inconsistencies. For example, an online fraud case might involve provisions from both the IT Act and general criminal law, which raises questions about which law should take precedence, or how they should be applied together.

There is also the issue of interpretation. Traditional criminal law was designed with physical acts in mind—things you could see, touch, or directly link to an individual. Translating those provisions into the digital context is not always straightforward. Courts and investigators often have to stretch definitions or rely on analogies, which, while practical, may not always be legally precise.[7]

2.3 Procedural Laws

If substantive law defines what constitutes a crime, procedural law determines how that crime is investigated and prosecuted. In India, the process is governed by the Code of Criminal Procedure, while the admissibility of evidence—especially electronic evidence—is regulated by the Indian Evidence Act.[8]Now, this is where things start to get particularly complex. Digital evidence does not behave like traditional evidence. It can be copied without altering the original, it can be tampered with in ways that are not immediately visible, and it often requires specialized tools and expertise to even access it. The law does recognize electronic records, but it also imposes certain conditions to ensure their authenticity and reliability.In practice, however, these conditions can become hurdles. Investigators may not always follow the correct procedures for collecting or preserving digital evidence. Something as simple as failing to maintain a proper chain of custody, or not obtaining the required certification, can render crucial evidence inadmissible in court. And when that happens, the entire case can weaken… sometimes beyond repair.[9]Another layer of difficulty comes from delays. Cyber forensic analysis can take time, especially when resources are limited. Courts, already burdened with heavy caseloads, may not always have the capacity to deal with technically complex cases efficiently. As a result, even strong cases can get stuck in procedural bottlenecks.

All of this points to a larger issue—the need for better integration between law and technology. It's not enough to have rules in place; those rules need to be understood, implemented correctly, and supported by adequate infrastructure. Until that happens, the gap between legal provisions and practical outcomes is likely to remain… and that's something that cannot be ignored any longer.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Nature of Cybercrime: A Forensic Perspective

Cybercrime at its core is not about computers or technology. It's really about how technology gets used and sometimes misused in ways that can harm people organizations and even entire systems.When we say cybercrime involves computers, networks or digital devices it sounds straightforward.. In reality it's more complicated than that. A single act, like a phishing attack or a data breach may involve devices, servers in different countries and layers of software working quietly in the background. You can't easily see it. Fully grasp it at first glance.What makes cybercrime different from crime is the kind of evidence it leaves behind. In crimes you might have physical clues like fingerprints, weapons and eyewitnesses. In cybercrime the evidence is often intangible. It exists in the form of data, like logs, metadata, IP addresses and fragments of deleted files. These things are not visible unless you know where and how to look.. Even then there's always some uncertainty.[10]Digital evidence can be altered, duplicated or erased easily without leaving any obvious trace. This makes investigating cybercrime feel like trying to piece a puzzle where some of the pieces keep shifting.

Another thing that complicates things is distance. Cybercrimes are not limited by geography. A person in one country can launch an attack on a system in another country using tools that hide their identity or location. This "remote execution" creates a kind of detachment between the offender and the offence. It's like the crime happens everywhere and nowhere at the time. For investigators this raises questions about jurisdiction cooperation between agencies and even basic issues like where to start. Then there's the side of things. Detecting and understanding cybercrime requires expertise that goes beyond policing. It involves knowledge of networks, encryption, operating systems. Sometimes even coding. Not every investigator has this training and even those who do may struggle with technologies that evolve faster than training programs can keep up. This gap between advancement and investigative capacity is a serious challenge in dealing with cybercrime. This is where digital forensics comes in and its role is crucial. Digital forensics is the process of identifying, collecting, preserving and analysing data in a way that is legally acceptable.. In practice it's more complicated than that. It involves handling of devices, specialized software tools and a constant awareness that even a small mistake can lead to loss of crucial evidence.One of the functions of digital forensics is to help identify perpetrators. This might involve tracing IP addresses analyzing login records or examining communication trails.. Identification is rarely straightforward. Offenders often use techniques like VPNs, proxy servers or anonymization tools to hide their tracks. So investigators are really building a chain of clues that point towards a particular person or group. It's a meticulous process and sometimes it leaves room for doubt.Another important aspect is data recovery. Deleting a file doesn't always mean it's gone forever. Digital forensics can often retrieve deleted or overwritten data, which can be critical in establishing what actually happened.. This depends on timing, tools and expertise. If much time has passed or if the data has been deliberately wiped using advanced methods recovery becomes harder.[11]Preserving evidence is equally crucial. Digital evidence must be collected in a way that maintains its integrity meaning it should not be altered or contaminated. This involves maintaining a chain of custody using forensic imaging techniques and documenting every step carefully. Courts demand a standard here. If there's any doubt about how the evidence was handled its admissibility can be. That can weaken the entire case.Tracing footprints is also important. Every action performed on a system leaves behind some trace. An access log, a timestamp, a transaction record. Digital forensics aims to reconstruct these traces into a narrative something that can be presented in court and understood by judges and lawyers who may not have technical backgrounds.. That's not an easy task. Translating technical

findings into something legally meaningful requires expertise, clarity and precision.All of this shows that cybercrime from a perspective is not just about catching offenders. It's about understanding a different kind of crime scene. One that is invisible constantly changing and deeply dependent, on technology.. While digital forensics provides the tools to navigate this space it also comes with its own limitations. This means the challenge is not just technological or legal. But a combination of both constantly evolving and never quite settled.

Challenges in Investigation of Cybercrime

Investigating cybercrime in India is different from investigating any crime. It doesn't start with a crime scene, visible evidence or direct human interaction. Instead, investigators deal with a space that's invisible, technical and constantly changing. The law provides some tools. The real challenge is using those tools effectively. That's where multiple difficulties start to appear… sometimes slowly sometimes all at once.

4.1 Lack of Technical Expertise

One of the challenges is the lack of technical expertise in law enforcement agencies. Investigating cybercrime is not about understanding the law; it requires knowledge of complex technological systems. This includes how data is stored, how networks work, how encryption works and how digital footprints can be traced. Many officers, at the local level are not trained in these areas.[12]It's not that they are not capable; it's just that they don't have the exposure and opportunity. Traditional police training focuses on crimes. Cybercrime units have been set up in regions but they are often limited in number and resources. Officers may struggle with tasks like recovering deleted data or understanding attack methods. Even handling a device without altering its contents requires specific knowledge.

There is also the issue of technological change. What an investigator learns today may become outdated in a years or even months. Keeping up with evolving technologies requires training, which is not always provided.

4.2 Inadequate Infrastructure

The problem of infrastructure is closely linked to the issue of expertise. Cyber forensic laboratories are essential for analyzing evidence but they are limited in India. Major cities may have access to facilities but many regions depend on a few centralized labs that are often overburdened with cases.This leads to delays… significant ones. Digital evidence needs to be analyzed to remain relevant and reliable. Backlogs can slow down the process. In some cases devices are sent for examination and remain pending for months. This can weaken the investigation. Affect prosecution later on.[13]The quality of infrastructure also varies. Advanced forensic tools and software are expensive. Require regular updates. Without investment laboratories may end up using outdated technology. This limits their ability to handle cyber offences.

4.3 Jurisdictional Issues

Jurisdiction is another area where cybercrime presents challenges. In offences jurisdiction is usually determined by the location where the crime occurred. In cybercrime this concept becomes blurred. A single offence may involve a victim in one state, an accused operating from another and servers located in a country.

This creates confusion about which agency should take the lead. While Indian law allows for extraterritorial applications enforcing these provisions in practice is not always straightforward. It often requires cooperation between states or even countries, which can be slow and complicated.[14]

4.4 Difficulty in Evidence Collection

Collecting evidence is a delicate aspect of cybercrime investigation. Digital evidence is highly volatile. It can be altered, deleted or overwritten easily. Investigators must act quickly. Also carefully. There is a tension between speed and accuracy. If evidence is not collected promptly it may be lost.. If it is

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

collected improperly it may become inadmissible in court. Maintaining this balance is not easy for officers who may not have specialized training.

4.5 Encryption and Anonymity

The use of encryption and anonymity tools complicates cybercrime investigations. Technologies like Virtual Private Networks (VPNs) and end-to-end encrypted communication systems allow users to conceal their identity and location.[15]These technologies serve functions from a privacy standpoint.. In the context of criminal investigation they create significant obstacles. Tracing an offender who has used layers of anonymization can be extremely difficult. The dark web has become a space where illegal activities can be conducted with secrecy. End-to-end encryption adds another layer of complexity. It ensures communication, for users but also limits the ability of law enforcement agencies to gather evidence.

Challenges in Prosecution of Cybercrime

Cybercrime at its core is not about computers or technology. It's really about how people use technology and sometimes misuse it in ways that can harm individuals, institutions and even entire systems.When we talk about cybercrime involving computers, networks or digital devices it sounds simple.. In reality it's much more complicated than that. A single act, like a phishing attack or a data breach can involve devices, servers in different countries and layers of software working in the background.[16]It's not something you can easily see or fully understand at glance. What makes cybercrime different from crime is the kind of evidence it leaves behind. In crimes you might find physical clues like fingerprints, weapons or eyewitnesses.In cybercrime the evidence is often intangible. It exists in the form of data like logs, metadata, IP addresses or fragments of deleted files. These things are not visible unless you know where and how to look.Even then there's always some uncertainty. Digital evidence can be altered, duplicated or erased easily without leaving any obvious trace. This makes investigating cybercrime feel like trying to piece a puzzle where some pieces keep shifting.Another thing that makes it complicated is the idea of distance. Cybercrimes are not limited by geography. A person in one country can launch an attack on a system in another country using tools that hide their identity or location.This "remote execution" creates a kind of detachment between the offender and the offence. It's like the crime happens everywhere and nowhere at the same time. For investigators this raises questions about jurisdiction cooperation between agencies and even basic issues like where to start.Then there's the side of things. Detecting and understanding cybercrime requires a level of expertise that goes beyond policing. It involves knowledge of networks, encryption, operating systems. Sometimes even coding.Not every investigator has this training and even those who do may struggle with technologies that evolve faster than training programs can keep up. This gap between advancement and investigative capacity is one of the quieter but more serious challenges in dealing with cybercrime. This is where digital forensics comes in and its role is crucial. Digital forensics is the process of identifying, collecting, preserving and analyzing data in a way that is legally acceptable. But saying it like that makes it sound more orderly than it is. In practice it involves handling of devices, specialized software tools and a constant awareness that even a small mistake can lead to loss of crucial evidence. One of the functions of digital forensics is to help identify perpetrators. This might involve tracing IP addresses analysing login records or examining communication trails.[17]Identification is rarely straightforward. Offenders often use techniques like VPNs, proxy servers or anonymization tools to hide their tracks. So investigators are really building a chain of clues that point towards a particular individual or group.It's a meticulous process and sometimes it leaves room for doubt. Another important aspect is data recovery. Deleting a file doesn't always mean its gone forever.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Digital forensics can often retrieve deleted or overwritten data, which can be critical in establishing what actually happened.. Again this depends on timing, tools and expertise.If much time has passed or if the data has been deliberately wiped using advanced methods recovery becomes harder.Preservation of evidence is equally crucial and perhaps one of the most delicate stages in the process. Digital evidence must be collected in a way that maintains its integrity meaning it should not be altered or contaminated.This involves maintaining a chain of custody using forensic imaging techniques and documenting every step carefully. Courts demand a standard here.[18]If theres any doubt about how the evidence was handled its admissibility can be. That can weaken the entire case. Then there's the idea of tracing footprints, which ties everything together.Every action performed on a system leaves behind some trace. An access log, a timestamp, a transaction record. Digital forensics aims to reconstruct these traces into a narrative that can be presented in court and understood by judges and lawyers who may not have technical backgrounds.That's not a task. Translating technical findings into something legally meaningful requires not just expertise, but also clarity and precision.All of this shows that cybercrime from a perspective is not just about catching offenders. It's about understanding a completely different kind of crime scene.One that is invisible constantly changing and deeply dependent, on technology.. While digital forensics provides the tools to navigate this space it also comes with its own limitations.Which means, perhaps that the challenge is not just technological or legal but a combination of both constantly evolving and never quite settled.

The Role of Digital Forensics in Cybercrime Cases

Digital forensics is really important for investigating and prosecuting cybercrime cases. It helps turn digital data into evidence that can be used in court. Without forensics it would be very hard to prove that a cybercrime happened. There might be some signs that something is going on but not enough to prove it in court.Digital forensics helps collect and preserve evidence. This can involve taking a computer making a copy of a drive or getting data from a mobile phone.. It is not as easy as it sounds. Every step has to be done carefully so that the data does not get changed. If the data gets changed, by accident it can make it hard to use as evidence later on. That is why it is so important to keep track of who handled the evidence when it was looked at and how it was stored. Courts look at this closely especially when it comes to the Indian Evidence Act, 1872.[19]Digital forensics also helps analyze the evidence. It allows experts to figure out what happened, when it happened and how it happened. There are techniques like making a copy of a storage device so the original data is not touched. There is also network forensics, which looks at data packets and finds activity on networks.. Then there is mobile device analysis, which is very important because so much personal and financial data is stored on smartphones. Email tracing is also important in cases of fraud or phishing.What makes these techniques so useful is that they can take data and turn it into something that can be understood in court. Forensic experts have to present their findings in court and explain things in a way that judges and lawyers can understand. This is a thing to do.

Digital forensics in India still has some problems. There is no way of doing forensic procedures, which can lead to differences in how evidence is handled. There are also not skilled experts. As cybercrime gets more complicated the need for trained professionals is growing, but there are not enough of them.[20]In the end digital forensics is an important part of investigating and prosecuting cybercrime cases. It is not a technical tool it is a crucial part of the justice process.. For it to work really well it needs more support, clearer rules and constant development. Otherwise it will not reach its potential. Digital forensics is key, to solving cybercrime cases and digital forensics is what

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

helps turn data into usable evidence.

COMPARATIVE

CONCLUSION

Cybercrime in India is a problem now. It is not something that happens to people. It is an issue that affects many parts of our lives. We see frauds and identity theft. We also see complex forms of cyber intrusion. The number and types of these crimes are growing. They are growing fast as technology is advancing. What makes cybercrime difficult to deal with is that it is always changing. New methods of cybercrime are emerging all the time. When we think we have a way to stop one type of crime another type appears. India has laws to deal with cybercrime. The Information Technology Act of 2000 is one of these laws. These laws are a start. They show that India recognizes the importance of regulating spaces. However the problem is not the laws themselves. The problem is how to implement these laws. Investigating cybercrime is not easy. One of the issues is that investigators often do not have the expertise they need. They also do not have access to the equipment. Sometimes it is not clear who should be investigating a crime. Cybercrime can involve people from different places. This makes it hard to know who is in charge. Collecting evidence of cybercrime is also difficult. Digital evidence is fragile. Can be easily altered. It requires care to collect and store. When we have evidence it can be hard to use it in court. The evidence has to be collected and stored in a specific way. If it is not it may not be allowed in court. Prosecuting cybercrime is also challenging. Courts have rules about what evidence can be used. This is a thing. However it can make it hard to win cases. Sometimes cases are lost because of mistakes. The people involved in the case may not fully understand the technology. This can make it hard to explain what happened. Despite all these challenges things are not hopeless. People are starting to recognize that cybercrime needs to be dealt with in a way. We need an integrated approach. This means that law and technology need to work. They are not things. They are connected. To move forward we need a plan. Our laws need to keep up with technology. We also need to provide training and resources for investigators and judges. We need to work with countries to share information and best practices. Cybercrime is not an Indian problem. It is a problem. We need a response.In the end dealing with cybercrime is not about having strict laws. It is, about creating a system that can adapt to change. We need a system that can understand and respond to types of crime. This is the way we can keep up with cybercrime. Justice depends on our ability to keep up with technology. This is the challenge we face.

Recommendations and Solutions

8.1 Capacity Building

- We need to develop training programs for police officers that focus on how to investigate crimes. These programs should teach them about evidence and the tools they need to do their job.
- We should also have courses for prosecutors so they can understand the technical side of cyber crimes and present their cases in court.
- Judges need to know about the cyber

technologies and how to use them to solve crimes.

- We should have teams that deal with cyber crimes in each district and state.
- Law enforcement agencies should work with institutions so they can learn from each other.

8.2 Strengthening Forensic Infrastructure

- We need laboratories that can analyze digital evidence.
- These labs should have the tools so they can handle new cyber threats.
- We need to make sure these labs have the money they need to stay to date.
- We should have rules for collecting and analyzing evidence so everyone does it the same way.
- We can work with companies to get the latest technology and expertise.

8.3 Reforms

- We need to make it easier to use digital evidence in court.
- We should update our laws to deal with types of cyber crimes like fraud and fake videos.
- We need to make it clear what laws apply to cyber crimes so prosecutors are not confused.
- We should have rules for handling evidence so it is done correctly.
- We should have courts that just deal with cyber crimes so cases can be heard quickly.

8.4 International Cooperation

- We need to work with countries to share information and evidence.
- We should have agreements with countries to help us investigate cyber crimes.
- We should participate in meetings to make sure our laws are in line with global standards.
- We should work with agencies to track down cyber criminals.
- We should have teams that deal with cyber crimes that cross borders.

8.5 Public Awareness

- We need to teach people about the dangers of crimes like phishing and identity theft.
- We should teach kids about cyber safety in school.
- We should have programs to help people, in areas learn about cyber safety.
- We should make it easy for people to report crimes.
- We can work with companies to teach people how to stay safe online and cyber crimes and cyber safety and cyber awareness and cyber threats and cyber security so people can learn about cyber crimes.

A. Books

Aparna Viswanathan wrote a book called Cyber Law: Indian and International Perspectives. It was published by LexisNexis in 2019.

Nina Godbole and Sunit Belapure wrote another book called Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. It was published by Wiley India in 2011.

There is also a book by Talat Fatima called Cyber Crimes. It was published by Eastern Book Company in 2016.

The Indian Cyber Laws is a book written by Suresh T Viswanathan. It was published by Bharat Law House in 2012.

Chris Reed and John Angel wrote a book called Computer Law: The Law and Regulation of Information Technology. It was published by Oxford University Press in 2007.

Majid Yar and Kevin F Steinmetz wrote a book called Cybercrime and Society. It was published by SAGE Publications in 2019.

Jonathan Clough wrote a book called Principles of Cybercrime. It was published by Cambridge University Press in 2015.

Cybercrime books like these are very helpful.

B. Journal Articles

K K Nair wrote an article called 'Cyber Crime Investigation and Digital Evidence' in 2020 for the Journal of Indian Law and Technology.

Brenner Susan W wrote an article called 'Cybercrime Investigation and Prosecution: The Role of Digital Evidence' in 2010 for the Murdoch University Electronic Journal of Law.

Wall David S wrote an article called 'The Transformation of Crime in the Information Age' in 2007 for Polity Press.

Ritu Kohli wrote an article called 'Cybercrime and Legal Framework in India' in 2018 for the International Journal of Law.

Arvind Narrain wrote an article called 'Regulating Cyberspace: The Indian Experience' in 2005 for the Indian Journal of Law and Technology.

C. Legislation

The Information Technology Act was passed in 2000.

The Indian Penal Code is a law that was passed in 1860.

The Code of Criminal Procedure is another law that was passed in 1973.

The Indian Evidence Act is a law that was passed in 1872.

The Digital Personal Data Protection Act is a law that was passed in 2023.

D. Case Laws

The case of Anvar P.V. V. P.K. Basheer was decided in 2014.

The case of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal was decided in 2020.

The case of Shreya Singhal v. Union of India was decided in 2015.

The case of State of Tamil Nadu v. Suhas Katti is another case.

The case of K.S. Puttaswamy v. Union of India was decided in 2017.

E. Government Reports & Publications

The National Crime Records Bureau publishes a report called Crime in India Report every year. It is published by the Ministry of Home Affairs.

The Ministry of Home Affairs has a scheme called Cyber Crime Prevention against Women and Children.

The Law Commission of India published a report called Report No 267.

The Indian Computer Emergency Response Team (CERT-In) publishes reports and guidelines about security.

The NITI Aayog published a report called National Strategy for Artificial Intelligence.

F. International Reports

The United Nations Office on Drugs and Crime (UNODC) published a report called Comprehensive Study on Cybercrime in 2013.

The Council of Europe published a report called Budapest Convention on Cybercrime in 2001.

The INTERPOL publishes reports about cybercrime strategy.

The World Economic Forum publishes a report called Global Cybersecurity Outlook.

G. Online Sources

The Ministry of Electronics and Information Technology (MeitY) has a website that's very helpful.

The National Cyber Crime Reporting Portal is a website where we can report cybercrime.

The INTERPOL has a website that provides information about cybercrime.

The United Nations Office on Drugs and Crime (UNODC) has a website that provides resources about cybercrime.

The Reserve Bank of India has a website that provides information about cyber security

framework for banks.

ENDNOTES

1 Ministry of Electronics and Information Technology, Digital India Programme (Government of India).

2 National Crime Records Bureau, Crime in India Report 2022: Cyber Crime Statistics (Ministry of Home Affairs).

3 Information Technology Act, 2000.

4 Ibid., s 66D.

5 Information Technology Act, 2000.

6 Indian Penal Code, 1860, ss 415, 420 (Cheating and Fraud).

7 Ibid., s 503 (Criminal Intimidation)

8 Indian Evidence Act, 1872, s 65B.

9 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

10 Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes (Wiley India 2011).

11 K K Nair, 'Cyber Crime Investigation and Digital Evidence' (2020) Journal of Indian Law and Technology.

12 Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes (Wiley India 2011).

13 Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis 2019).

14 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

15 K K Nair, 'Cyber Crime Investigation and Digital Evidence' (2020) Journal of Indian Law and Technology.

16 Indian Evidence Act, 1872, s 65B; Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

17 National Crime Records Bureau, Crime in India Report (latest available edition).

18 K K Nair, 'Cyber Crime Investigation and Digital Evidence' (2020) Journal of Indian Law and Technology.

19 Indian Evidence Act, 1872, s 65B.

20 Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes (Wiley India 2011).