National Judicial Academy, Nepal
(Estd. under the National Judicial Academy Act, 2006)
Manamaiju, Kathmandu
Tel: 977-1-4027449/4027451, Fax: 977-1-4027140
GPO Box No: 24865
Email: info@njanepal.org.np
URL: www.njanepal.org.np

A Study on CYBER CRIME Cases in Nepal

CHALLENGES AND RECOMMENDATIONS 2022

National Judicial Academy, Nepal
Manmaiju, Kathmandu

A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations

2022

National Judicial Academy, Nepal
Manmaiju, Kathmandu

Researchers

Advocate Ashankan Malla

Advocate Rastra Bimochan Timalsena

Publisher

National Judicial Academy, Nepal

Manamaiju, Kathmandu, Nepal

PO Box No.: 24865

Tel: 977-1-4027499/4027451

Printed at: Naba Print Solution

Note: The contents and data presented in this report are solely of the researchers. They are not necessarily the views of the NJA-Nepal.

Preface

Internet as a system has been around for more than 50 years but its growth to what it is now happened in last 25 years. This sort of change is unprecedented. However, when we look into Nepal's history of internet, the change is even more rapid. We went from a country with 10% people being able to access to internet to 68% within a decade. While this has led to positive changes, this rapid development has also opened up Pandora's Box. It has always seemed that the Nepalese legal system and Nepal's law is playing catchup with technology and Nepal's law has not been able to address various problems related to cyberspace, cyber security et al. The researchers here have looked into these problems, specifically, the problems faced by the Judiciary while trying to solve issues pertaining to cyberspace.

The problems and crimes brought by or in sector of information technology/ internet have virtually no boundaries. This study is significant as it traces out the situation of cyber laws, cybercrimes, and status of cyber cases in Nepalese court and statistically analyse these cases so as to recommend the concern agencies to ensure that the cyber laws in Nepal are up-to-date and also to ensure easy and proper judgment in cyber law cases. The researcher believes that the final paper will provide the readers with knowledge of cybercrimes prevalent in Nepal, cyber laws cases of Nepal, how these cases are adjudicated in Nepal and the attitude to judiciary in Cyber law cases.

The researchers here would like to thank National Judicial Academy for providing an opportunity to write a research paper in this area which, in Nepal, there is dearth of information and data. The

researcher here would also like to thank Mr. Shrikrishna Mulmi for his continuous support and guidance throughout this report writing endeavour. Further, we would like to extent our gratitude and appreciation towards our interns and researchers who helped in collection of data and information, without whom this research would not be possible. Additionally, it is equally vital to remember the contribution of experts in this field, from defence attorney, government attorney, investigation officers and district court judges who helped in making of this paper by providing their valuable input and ideas by sharing their experience.

राष्ट्रिय न्यायिक प्रतिष्ठान, नेपाल
National Judicial Academy, Nepal
(Estd. under the National Judicial Academy Act, 2006)
"... Centre of Excellence for Judicial Education."

Message

Cyber Space is one of the amazing human creations of the 21st century. With the advancement of the cyber space that is information and communication technology, the globe has become a small village. Sharing of the news, views and ideas within a flip of second has become possible because of this invention. Moreover, in our day today life like banking transection, shopping, bill payment, online services mail correspondence, etc. has made our life easy and comfortable. However, while using this useful invention, there is high risks and threats as well. Various cyber related crimes such as vishing, phishing, hacking, cyber extortion, data breach, identity theft, harassment, defamation, stalking, fraud and so on have become a serious problems and are quiet challenging also. They are sometime against people, sometime against properties and even sometimes against Government. Because of its complex nature, it is very difficult to determine these cases during investigation and prosecution and also in the court as well while making decision. The cyber-crime is not only a national problem, but this problem is also challenging in the international arena.

Against the backdrop, a research paper titled 'A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations' is being published under the flagship of the National Judicial Academy (NJA), Nepal. The report is detailed and analytical on the concept and ideas of the cybercrime, its types, existing legal instruments, nature, trends and working mechanism in the field of cybercrime cases in Nepal. At the very outset, I would like to congratulate the researcher Advocate Mr. Ashankan Malla and Advocate Mr. Rastra Bimochan Timalsena for their hard work and dedication in making this incredible research report. Further, I would like to extend sincere thanks to Deputy Executive Director Hon. Kedar Paudel, Faculty/District Judge Dr. Diwakar Bhatta, Director Mr. Shreekrishna Mulmi and Deputy Director Mr. Sanjib Rai and entire NJA team for their guidance, feedback, inputs and patience to shape the research paper in its present form. I hope the paper will be a mile milestone in the area of the cyberspace and cyber-crime in the Nepali context.

मनमैजु, काठमाडौं
फोन नं.: +१-४०२७४४९, +१-४०२७४५१
फ्याक्स +१-४०२७१४०
पोष्ट बक्स नं.: २४८६५

E-mail : info@njanepal.org.np
URL: www.njanepal.org.np

Manamaiju, Kathmandu
Ph.: +1-4027449, +1-4027451
Fax: +1-4027140
Post Box No: 24865

राष्ट्रिय न्यायिक प्रतिष्ठान, नेपाल
National Judicial Academy, Nepal
(Estd. under the National Judicial Academy Act, 2006)
"... Center of Excellence for Judicial Education."

This research work is very timely and would obviously help to pave the way for the further research in the area of the cyber space and cyber security which is very relevant and significant issue at the present contest. I have a strong belief that the issues raised in this research paper would be insightful for judges, lawyers, government attorneys and all other stakeholders engaged in the areas of the law and justice.

.....

Baidya Nath Upadhyay
Executive Director

मनमैजु, काठमाडौं
फोन नं.: +१-४०२७४४९, +१-४०२७४५१
फ्याक्स +१-४०२७१४०
पोष्ट बक्स नं.: २४८६५

E-mail : info@njanepal.org.np
URL: www.njanepal.org.np

Manamaiju, Kathmandu
Ph.: +1-4027449, +1-4027451
Fax: +1-4027140
Post Box No: 24865

Table of Contents

Background of the Study

"Keeping people safe online is an enormous task, and no one entity or government has the perfect solution. But there is much we can do, and need to do more of, to strengthen prevention and improve responses to cybercrime."

- *Yury Fedotov, Executive Director of the UNODC*

The modern world is changing into a global village, a single window that can connect one single person to the whole world. Around the world, societies are becoming increasingly dependent upon information and communications technology (ICT), driving rapid social, economic, and governmental development. As of January 2021, there were 4.66 billion active internet users worldwide - 59.5 percent of the global population.[1] Of this total, 92.6 percent (4.32 billion) accessed the internet via mobile devices, with 4.2 billion active social media users.[2] Along with this development, new threats to digital infrastructures and opportunities for misuse of cyberspace have emerged, affecting individuals, society, and governments alike.

Cybercrime is one of the fastest-growing areas of criminal activity. Advancement in the information technology (IT) sector resulting in the rapid growth in computer and internet users has not only led to its development but has also led to a rise in criminal activities and misuse of computer technology, posing new types of challenges for the justice delivery system. Criminals use modern information technology as it offers speed, convenience, and anonymity. Social media harassment, online defamation, internet fraud, email scams, identity theft, breach of privacy, abuse of personal data, and attacks against computer data and systems are a few

[1] International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database https://data.worldbank.org/indicator/IT.NET.USER.ZS

[2] *Id.*

examples of cybercrimes. Furthermore, due to the global and adaptive nature of the internet, criminal activities anywhere in the world in a variety of ways have made all countries enact and enforce strong and holistic cyber laws.

Nepal is not free from the threat of cybercrime. The internet users in Nepal have been rampantly increasing. According to the data collected from the World Internet Stats, there are almost 22 million internet users in Nepal,[3] a steep jump from having only fifty thousand internet users[4] at the turn of the millennium. This denotes a 73.8% penetration rate of internet users out of its total population. Further, there are around 12.3 million Facebook users in Nepal,[5] the most popular online social media platform globally. Such a rise in Internet users would inevitably increase criminal activities as Internet platforms provide criminals with anonymity coupled with distance proximity. However, with limited policies and regulations and an ever-increasing number of offenses carried out online, Nepal's legal institutions face several challenges in dealing with cybercrime cases.

The Electronic Transactions Act 2063 (ETA) regulates cyber activity in Nepal, which primarily seeks to protect internet users against cybercrimes. The ETA does not specifically define cybercrimes but does provide for various provisions that deal with the issues about such crimes. Unfortunately, the provisions of this Act are vague and are not comprehensive enough to address the varied challenges associated with complaints, investigation, prosecution, and adjudication of cybercrimes in Nepal. In this light, the Government of Nepal has tabled the Information Technology Bill and the Cyber Crime Bill before the Parliament.

---

[3] Internet World Stats – Usage and Population Statistic, *Nepal*, (2013), http://www.internetworldstats.com/asia/np.htm

[4] *Id.*

[5] *Supra note* 3.

Under the existing regime, some gaps and discrepancies pose great challenges to the proper implementation and enforcement of the law. Moreover, Courts face unique obstacles while adjudicating cases relating to cybercrimes. These challenges have been amplified because, at present, all the cybercrime cases in Nepal must be prosecuted at the Kathmandu District Court though the ETA recognizes the need for a specialized court to carry out the proceeding and adjudication of cybercrime cases. In addition, the practice of centralized jurisdiction has created limited access to justice and overwhelmed the district court with a high volume of cases. These problems have become even more prominent during the COVID-19 pandemic due to the increasing number of cybercrimes during this time.

It is therefore important to study and understand the challenges through the lens of the Court. By identifying and highlighting the gaps and weaknesses in the legal framework relating to cybercrimes in Nepal, we can better address the said institutional problems and accordingly identify comprehensive measures for the effective handling of cybercrime cases. The purpose of this paper shall be to deal with the following issues:

- to determine and analyse cases pertaining to cybercrimes in Nepal (with data) and the nature of such cases.
- to identify the strengths and weaknesses in the criminal justice delivery system (investigation, prosecution, and adjudication) to deal with cybercrime cases under the existing legal system.
- to highlight the challenges faced within the criminal justice delivery system concerning cybercrime cases.
- to recommend enforceable and holistic solutions to the said challenges based on the findings and observation of the study.

Research Methodology

Research Questions

1) How effective is the existing legal framework for cases pertaining to cybercrimes in Nepal?
2) What are major challenges faced by the Kathmandu District Court while adjudicating cybercrime cases in Nepal?
3) What improvements can be made for the effective administration and adjudication of cybercrime cases at the Kathmandu District Court?

Research Methodology:

This paper is based on a doctrinal as well as empirical research methodology using primary and secondary sources of data of research, whereas data has been collected using qualitative and quantitative data. For primary resources, the Researchers have relied on decisions of the Court, FIR and Charge sheets, Legislative Arrangements, and Regulatory frameworks. In addition, the Researchers have also relied on interviews of key stakeholders (informants), such as Judges, public prosecutors, Lawyers, Police, Cyber Bureau, lawmakers, Experts, ISPs, victims, and Accused/Perpetrators. As for the secondary sources, the Researchers have studied and reviewed various Books, Articles, Publications, Reports, and Government Databases.

Scope and Limitation

The scope of this paper is limited to the study of cybercrime cases registered at the Kathmandu District Court to identify and highlight the difficulties in the investigation, prosecution, and adjudication. The paper will refrain from undertaking an in-depth analysis of the various concepts and categories of cybercrimes. With regard to identifying and highlighting the problems and challenges of cybercrimes in Nepal, the researcher shall focus on the issues and challenges faced by the criminal justice delivery system – Police,

Lawyers, and Judges. The statistics of cases collected from Kathmandu District Court are till 2078 B.S however, the cases analysed in-depth from the data collected is until 31 Chaitra 2076 BS due to the unavailability of files and documents of ongoing cases.

The cases identified for analysis are sampled and selected based on the nature, novelty, modus operandi, popularity, magnitude, and difficulties courts face while adjudicating. Some cases are simply based on random sampling. Data presented in this paper may not be 100% accurate since data were collected manually from individual cases registered in the Kathmandu District Court.

Mode of Writing

The Researchers have relied on a Comparative, Analytical, and Descriptive way of writing.

Chapterization

- **Chapter 1:** The first chapter of this paper shall narrate the meaning, nature, scope, and concepts of cybercrimes and further classify the various types and trends of cybercrimes.
- **Chapter 2:** This chapter explores Nepal's existing legal framework on cybercrimes, including the complaint registration mechanism, focusing especially on the Electronic Transaction Act, 2008.
- **Chapter 3:** This chapter makes a detailed study of the nature, extent, situation, and trends of cases relating to cybercrimes in the Nepali context. Here, the researchers have conducted a thorough analysis of the cases registered under the ETA and adjudicated by the Court in order to identify the effectiveness of the criminal justice delivery system.

- **Chapter 4:** This chapter investigates and highlights the major problems and challenges faced by the criminal justice system (investigation, prosecution, and adjudication) in dealing with cybercrime cases in Nepal.
- **Chapter 5:** This Chapter shall build upon the critical analysis done in the previous chapter, propose holistic solutions, and make recommendations for better implementation and formulation of the laws and effective administration and adjudication of cyber cases by Courts.

Chapter 1

Cyber Crimes – A Conceptual Framework

Cybercrime is a set of criminal activities perpetrated using the computer system and the internet. Cybercrime refers to various crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, game consoles, and smartphones. It is also defined as a technology-enabled crime, IT crime, digital crime, electronic crime, virtual crime, internet crime, and high technology crime. According to Halder & Jaishankar,[6] "Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental hurt, or loss, to the victim directly or indirectly, victimization trendy telecommunication networks like the Internet."

Cyber Crime is an act of creating, distributing, altering, stealing, misusing, and destroying information through the computer manipulation of cyberspace.[7] As per Black's Law Dictionary: "crimes that take place through computers, computer technology or the Internet is known as Cyber Crime."[8] Cybercrime refers to criminal activities within cyberspace, i.e., happening in the world of computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts, from hacking and identifying theft to data breach and data diddling. Cybercrime also includes other non-monetary offenses, such as creating and distributing viruses, posting confidential or derogatory

[6] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women in India*, 2017.
[7] M Dasgupta, *Cyber Crimes in India: A Comparative Study*, 2009.
[8] Definition from The Law Dictionary website: https://thelawdictionary.org/Cybercrime .

content/information on the Internet, or online harassment and cyberbullying.

One of the fastest-growing areas of criminal activities, cybercrimes involve unlawful acts where the computer is used either as a tool or a target or both. The advancement and reach of technology worldwide and the enormous growth in the use of computer devices have led to an increase in incidents of cybercrimes. This includes a range of crimes against an individual, business community, society, or government, including but not limited to online harassment and defamation, data leaks and unauthorized access, hacking and digital theft, copyright infringement and fraud, and cyber terrorism and cyber warfare.

The European Convention on Cybercrime 2001, commonly known as the Budapest Convention, has listed offences relating to illegal access, illegal interception, data interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and copyright infringements as cybercrimes. However, the criminal offences that constitute cybercrime are not clearly developed and defined anywhere, and there is no exhaustive list providing all sets of cybercrimes.

Cybercrimes are mostly the expansion of traditional crime with the support of modern technology i.e., cyber-enabled crime. Such traditional or conventional crimes made easier by using computers are known as cyber-enabled crimes. Cyber-enabled crime is a crime that can take place offline but is made easier by the advent of internet and computer technology[9]. From white-collar crime, such as fraudulent financial transactions, identity theft, and the theft of electronic information for commercial gain, to drug trafficking, child exploitation, harassment, stalking, and other dangerous behaviours, the variety of cyber-enabled crimes is vast. The use of the

[9] United Nations Office on Drugs and Crime, *Global Programme on Cybercrime*, UNODC, (date of visit 05-20-2022), https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

internet and communications technology has revolutionized the scale and shape of cyber-enabled crimes, which are not dependent on computers or networks[10]. On the other hand, cyber-dependent crimes are ones that would not be possible without the use of cyber technology. Illicit incursions into computer networks, such as hacking, disruption, or lowering computer capability and network space, such as viruses and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks, are examples of cyber-dependent crimes[11]. A cybercriminal can use the internet to cause massive commercial damage.[12] The work of the hacktivist is one of the modern incarnations of cyber-dependent crime. The 2010 Anonymous hacktivist attack on Mastercard, Visa, and Paypal in retaliation for their refusal to transmit donations to the WikiLeaks group is one of the recent memorable examples of cyber-dependent crime.

The evolution of Information Technology (IT) gave birth to the cyber space wherein the internet provides connectivity and anonymity to individuals and groups, including those with *mala fide* intent. The problem arises when these individuals access the internet from any part of the world to harm or hurt another person or entity. Since borders between counties in cyberspace have become obscure, these crimes have acquired a transnational characteristic, as they are committed across a non-physical space, having real-world consequences. Thus, cybercrimes have an international aspect for making regulation much more difficult for national governments.

Cybercrime encompasses a wide range of activities, but in general, it has three categories:

---

[10] Ron Alvarez, Cyber Enabled Crime vs. Cyber Dependent Crime, IPPROBE.GLOBAL, (date of visit05-20-2022),https://ipprobe.global/2021/09/02/cyber-enabled-crime-vs-cyber-dependent-crime/#:~:text=%E2%80%9CCyber%2Denabled%20crime%20is%20traditional,ransomware%2C%20DDoS%20attacks%20and%20malware.

[11] *Id.*

[12] https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

i) Computer Target: The crime in which a computer is the target of the offense. Offenses against the confidentiality, integrity, and accessibility of computer data and systems fall. Obtaining unauthorised access to a computer or computer system, causing unauthorised damage or impairment to computer data or the operation of a computer or computer system, or the illegal interception of computer data are all examples of activity that these offences seek to address. These crimes include using a computer to obtain information or cause damage to operating systems, such as theft of intellectual property, theft of marketing information, and blackmail based on information gained from computerized files.[13]

ii) Computer Medium: the crime in which a computer is used as a tool or medium in committing the offense. Computers are used as an instrument to further illegal ends by gaining access to sensitive data such as passwords, credit card numbers, and other sensitive data for malicious or exploitative purposes such as fraud, trafficking in child pornography and intellectual property, stealing identities, or violating identities privacy. Acts of fraudulent use of automated teller machine (ATM) cards and accounts, theft of money from accrual, conversion, or transfer accounts, credit card fraud, fraud from computer transactions (stock transfer, sales, or billing), and telecommunications fraud also fall under this category.

iii) Computer Incidental: the crime in which a computer plays a minor role in committing the offense such as money laundering and

[13] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 31 – 55 (Cambridge University Press, 2nd eds, 2015).

unlawful banking transactions, organized crime records or books, and bookmaking.

Thus, any activity that uses computers as an instrument, target, or means to perpetrate a further crime falls within the ambit of cybercrime. This explanation, however, focuses more on the functional aspects of criminal activity rather than envisaging a universal legal definition. There is also a fundamental need to distinguish between pure cybercrime and an electronically enabled crime. A pure cybercrime is a malicious act not capable of being perpetuated outside of the online environment. An electronically enabled crime is a criminal act known to the world even before the coming of the internet age.[14]

The increase in internet traffic has triggered a higher proportion of legal issues worldwide. Because cyber laws vary by jurisdiction and country, enforcement is challenging, and restitution ranges from fines to imprisonment and, in some instances, compensation. In addition, the rapid development of information technology has created new challenges in the law that are not confined to a particular category of law but arise in diverse areas, such as criminal law, intellectual property law, contract, and tort. Due to the rapid development of the internet and the World Wide Web, various unprecedented problems have emerged. These problems concern the issues of free speech, intellectual property, safety, equity, privacy, e-commerce, and jurisdictional challenges.[15] Challenges to cybercrimes have been discussed in detail in Chapter 4 of this Paper.

Cybercrime is an emerging trend of modern crimes around the globe with a unique modus operandi - the method acquired by any criminal for the successful commission of a crime. The modus operandi depends on a case-to-case basis where the perpetrator uses several modes of technology to

[14] Creole Palmer et al, *Cyber Crime – A New Breed of Criminal*, 2003.
[15] Dr. Tarbez Ahmed, *Nature and Scope of cyber law*, 2018.

commit the crime. A skilled and determined cyber-criminal can use multiple entry points to navigate around defences, breach your network in minutes and evade detection. For every type of cyber offence, the perpetrator may adopt a different modus operandi. For example, to commit crimes of harassment and defamation, the perpetrator may use the medium of online texting, social media platforms, or online news portals. Likewise, a person may make fake profiles in social media and websites to commit internet fraud. Where previously, illegal access to a computer system was committed by accessing the respective system, now, due to the advent of cloud computing, the perpetrator can access the data via a cloud system. Therefore, due to the modern nature of cybercrimes, the modus operandi of committing such offences may constantly be evolving.

Types of Cyber Crimes

A formal and comprehensive classification and categorization of the various types of cybercrimes is a difficult task. Moreover, every day from different corners of the world, there are new kinds of cybercrime issues and challenges, making every effort to prevent it almost futile. Nevertheless, the United Nations Office of Drugs and Crime has attempted to categorize cybercrime broadly into three areas[16] such as:

(i) Acts against the confidentiality, integrity, and availability of computer data or systems,

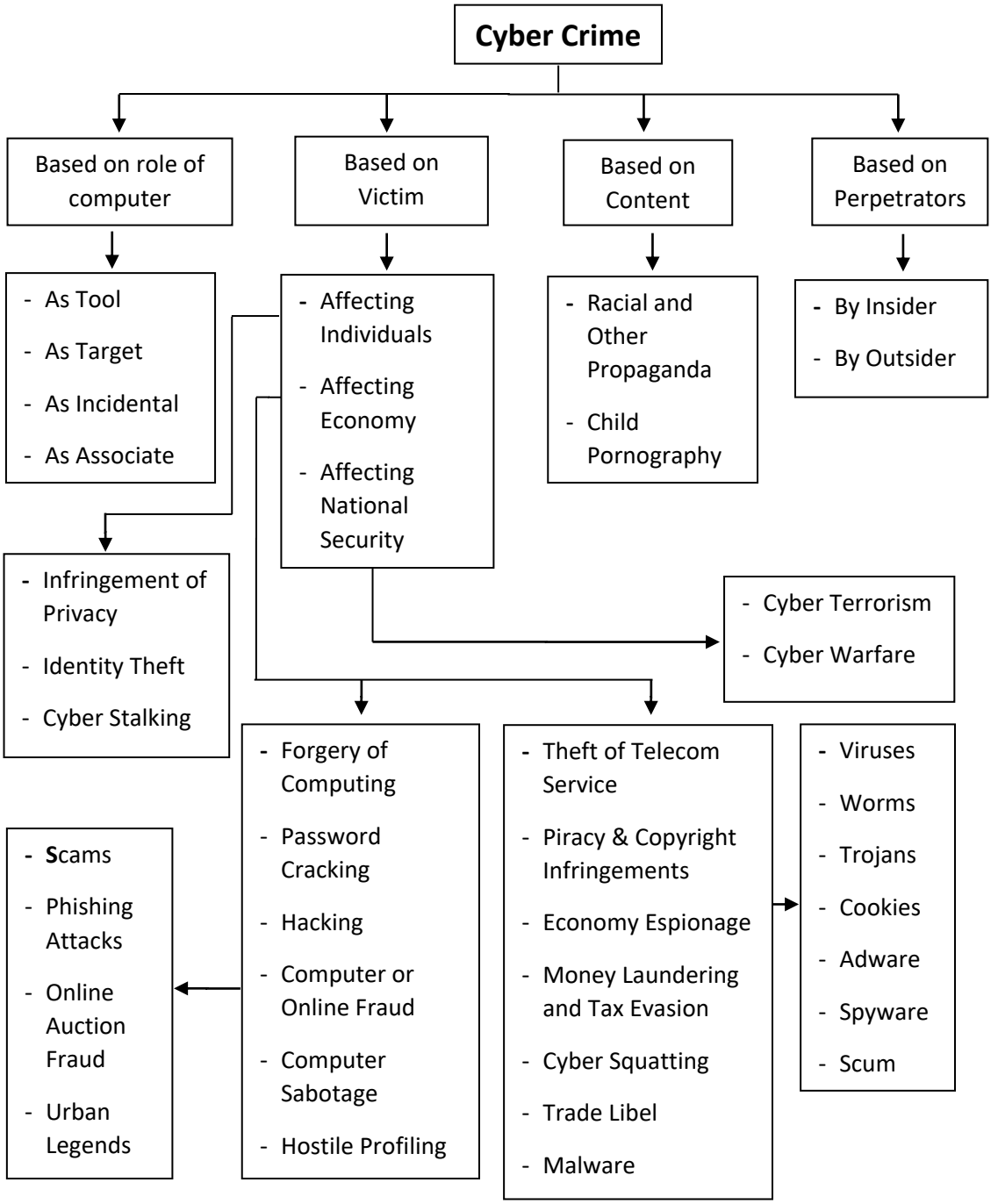
(ii) Computer-related acts for personal or financial gain or harm and

(iii) Computer content-related act.

Although there are some intersections with categorization, in general practice, cybercrimes can be classified based on four different factors – i) the role of the computer; ii) targeted against a victim, iii) nature of the content;

[16] Phulara, Bashu Dev,*Crime: Tackling Cybercrime in Nepal*, In: The Nepal Digest, Newyork, year 15 volume XI, issue 1 (November 24, 2004).

and iv) perpetrators or persons involved. This classification is shown in the illustration below: -



In addition to the above, cybercrimes can be further classified the on the following basis:

i. **Cyber Crimes against Individuals**

- Cybercrimes committed against any individual persons – legal and natural persons – such as offences relating to online defamation, blackmails, email bombings, cyberbullying, social media harassment, indecent exposure, hacking, fake profiles and false identity, the transmission of child pornography, data infringements, phishing, online scams, identity theft, computer fraud, etc.

ii. **Cyber Crimes against Property**

- Crimes target the computer system to damage or destroy the computer or computer data, such as Computer Vandalism; Destruction of Data; Software Piracy; Transmission of harmful programs; ATM theft; Siphoning of funds from financial institutions; Stealing/Leaking secret information & data, etc.

iii. **Crimes against Society and Public Morality**

- Criminal activities that disturb peace and order create a public nuisance or threaten public morality, including Publication of Indecent Content, Dissemination of Fake news, Grooming, Sale of Illegal Articles, Online Gambling, Fraud, Forgery, etc.

iv. **Crimes against Government**

- Crimes committed through the internet target nation, states, and governments to achieve political or ideological gains through threats and intimidation, such as Cyber terrorism, Cyberwarfare, Cyberespionage, Cyber extortion, Hacking into Government databases, etc.,

At the outset, it should be noted that it is an impossible task to list all the numerous categories of cybercrimes as they differ in terms of constituent elements and methods – modus operandi. However, this chapter was a sincere attempt by the Researchers to identify and classify the various cybercrimes based on general international practice. Furthermore, the Researchers have delved more deeply into the recurring themes of the types and trends of cybercrimes experienced in Nepal in the subsequent chapters of this paper.

Chapter 2

Legal Mechanism relating to Cyber Crimes in Nepal

The Constitution of Nepal 2072 provides that the State shall pursue development policies that ensure – a) the development and expansion of the national information technology framework to fulfil the needs of the nation, b) easy and simple access to information technology for the general public, and c) optimal usage of the information technology framework for national development.[17] Cybercrimes are a relatively new phenomenon in Nepal, as the internet was introduced in Nepal only in 1994. Still, due to the development and proliferation of the information technology framework in Nepal, the internet has reached the majority of the places in Nepal. Prior to 2008, offences relating to cybercrimes were dealt with by the Muluki Ain, Some Public (Crime and Punishment) Act 2027, and the Telecommunications Act 1997. However, as cases related to cyber offences became prominent and pressing, there was a need for a law to govern cyber law issues specifically. As such, the ETA 2063 BS was introduced and promulgated on 24th Bhadra 2063.

The Electronic Transactions Act, 2063:

The Electronic Transaction Act (hereinafter called ETA), 2063, is the first comprehensive legal instrument that specifically regulates cyber space in Nepal. This Act was established to create legal provisions for authentication and regularization of the recognition, validity, integrity, and reliability of the generation, production, processing, storage, communication, and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of

[17] Constitution of Nepal, 2072, art. 51 (f) (5).

electronic communications, reliable and secured, and also for controlling the acts of unauthorized use of electronic records or of making alteration in such records through an illegal manner.[18]

The term cybercrime(s) has not been defined in the Act. However, certain terminologies like "Computer," "Computer Database," "Computer Network," "Computer System," "Data," "Access," "Information and Information System," "Electronic Records," "Software," and "Computer Accessory" – which are used as a medium or target of cybercrimes – have been defined under this Act.[19] On the whole or part, the ETA deals with provisions relating to electronic records and digital signatures, controller and certifying authority, digital signatures and certificates, subscriber's duties and rights, government use of digital signature, network service, and the constitution and composition of tribunals. In addition, chapter 9 of the Act deals with Offences Relating to computers, which can thematically be classified as Cybercrimes in the context of Nepal's legal mechanism.

Below is a list of the most prosecuted offences under the ETA:[20]

Section No.	**Nature of Cyber Crime**	**Elements of Cyber Crime**	**Punishment**
44	To pirate, destroy, or alter the computer source code	To pirate, beat, or alter the computer source code of any computer, computer program, computer system, or computer network knowingly or with *mala fide* intention.	Fine not exceeding two thousand rupees, or with imprisonment not exceeding three years, or with both depending on the seriousness of the offence.

[18] ETA 2008, Preamble.
[19] ETA 2008, § 2.
[20] ETA 2008, chapter 9.

45	Unauthorized access to computer materials	To use the computer without authorization of the owner or the person responsible for such a computer. To have access to any program, information, or data contrary to such authorization.	Fine not exceeding two thousand rupees or with imprisonment not exceeding three years, or both.
46	Damage to any computer and information system	To destroy, damage, delete, alter, or disrupt any information of any computer source, diminish the value and utility of such information, or affect it injuriously. Knowingly and with a *mala fide* intention to cause wrongful loss or damage	Fine not exceeding two thousand rupees or with imprisonment not exceeding three years, or both.
47	Publication of illegal materials in electronic form	To publish or display any material in the electronic media, including computer, internet which are prohibited from being published or displayed; be contrary to the public morality or decent behavior; spread hate or jealousy against anyone;	Fine not exceeding one Hundred Thousand Rupees, or with imprisonment not exceeding five years, or both. Recidivist Offender: liable to the punishment for each time with one-and-one-half

		or jeopardize the harmonious relations subsisting among the peoples of various castes, tribes, and communities.	percent of the previous punishment.
48	Confidentiality to divulge	To divulge or cause to divulge confidentiality to any unauthorized person.	Fine not exceeding ten Thousand Rupees, or with the imprisonment not exceeding two years, or with both.
52	To commit computer fraud	To create, publish, or otherwise provide a digital signature certificate, or acquire benefit from the payment of any bill, the balance amount of anyone's account, inventory, or ATM card with an intention to commit fraud or any other illegal acts.	Fine not exceeding one hundred thousand rupees, or with the imprisonment not exceeding two years, or both.
53	Abetment to commit a computer-related offence	To abet others to commit an offence relating to computers, attempt, or be involved in a conspiracy to commit such an offence.	Fine not exceeding Fifty Thousand Rupees, or with the imprisonment not exceeding six months, or both depending on the degree of the offence.

54	Punishment to the Accomplice	To assist others in committing any offence under this Act or acting as an accomplice.	Half of the punishment for which the principal is liable.
57	Offences Committed by Corporate Body	An act done by a corporate body is deemed an offence under this Act.	Deemed to have been committed by a person responsible as chief for the operation of the corporate body at the time of committing such an offence. Director, manager, secretary, or any other responsible person of such a corporate body may also be held liable if it is proved that such a person had the knowledge of, or gave the consent for, or caused by way of negligence, the offence under this Act committed by the corporate body.

As outlined in the Table above, cybercrimes under the ETA range from piracy to unauthorized access, damage to computer systems, publication of illegal materials online, etc. The various types of cybercrimes laid down are backed by sanctions as per the gravity of offence and nature of the crime. However, in addition to the punishment of imprisonment and fine, the ETA also provides compensation to be recovered by the victim of crime for any loss or damage caused to them due to the commission of such offence under this Act.[21]

The Act has stipulated extra-territorial jurisdiction in cases of cybercrimes, *i.e.*, if any person commits any act which constitutes an offence under the ETA and which involves the computer, computer system, or network system located in Nepal, even though such an act is committed while residing outside of Nepal, a case may be filed against such a person and shall be punished accordingly.[22] Furthermore, under Section 59 of the ETA, the Act does not pose any limitations to trying cybercrime offences that can be specifically tried under other existing laws. It stipulates that any act deemed to be an offence under this Act is also considered offences under other prevailing laws. Therefore, any hindrance shall not be caused under the ETA to file separate cases accordingly[23]. For example, online fraud or online theft cases can be tried under penal laws of fraud and theft, respectively. Similarly, defamation cases can be tried as per the provision on defamation under the Muluki Penal Code. The ETA provides a statutory time-limitation of thirty-five days to file complaints.[24]

Finally, in order to try and prosecute cybercrime cases, the ETA prescribes the establishment of an Information Technology Tribunal.[25] However, the Act

---

21 ETA 2008, §76.
22 ETA 2008, §55.
23 *Id.* at §59.
24 *Supranote* 22, at §76.
25 *Supranote* 22, at §60(1).

provides that until the IT Tribunal is constituted, all proceedings and adjudication of cybercrime cases shall be filed at the Kathmandu District Court.[26]

Information and Communication Technology (ICT) Policy 2072

The Nepalese government established the Information Communication Policy 2072(2015) in response to a call for a revised policy encompassing all aspects of information and communication technology. This strategy emphasizes the importance of a well-defined and consistent legislative and regulatory framework for dealing with the converging telecommunications, television, and information technology regimes.[27] This policy is based on realizing that strategic responses to technical developments impacting the ICT sector are urgently needed. This policy is intended to lay the groundwork for an overarching vision of Digital Nepal. Timely and cost-effective public service delivery through an online system, a better communication channel between government sectors, and accountability and transparency are some expectations from this policy.

CERT Guidelines, 2075

The government has established the National Computer Emergency Response Team to respond to computer and network security incidents, report vulnerabilities, and encourage effective ICT security practices across Nepal. It is an expert group that deals with computer security events and educates people about cyber security in Nepal[28]. CERT Nepal is in charge of improving the cybersecurity posture of the nation, coordinating cyber

---

[26] *Supranote* 22, at §60(5).

[27] Roopali Bista , *ICT for Improving Governance in Nepal*, SAMRIDDHI ORGANIZATION, (date of visit 05-14-2022),https://samriddhi.org/news-and-updates/ict-for-improving-governance-in-nepal/#:~:text=2072%20(2015).,This%20policy%20stresses%20in%20the%20need%20for%20a%20well%2Ddefines,information%20communication%20technology%20in%20Nepal.

[28] Nepal CERT, *About Nepal CERT*, NEPAL CERT, (date of visit 05-20-2022), https://www.nepalcert.org.np/

information sharing, and proactively managing cyber risks to the country while safeguarding Nepalese citizens' constitutional rights.

CERT was established with the aim towards providing and promoting cyber security responses and awareness, publishing security threat alerts, performing information security audits and assurance, conducting cyber security research and training, performing analysis and forensic investigation of cyber incidents, responding to cyber security incidents, and coordinating with global and local agencies toward cybercrime.[29] However, the lack of certified security professionals and lack of awareness and knowledge among the people, and executives, can be challenges for the effective functioning of CERT in Nepal.

Constitution of Nepal, 2072

The Constitution of Nepal 2072 has guaranteed certain fundamental rights, which also have significant relevance with the right to information and privacy though indirect with cyber space. These fundamental rights include freedom of opinion and expression,[30] right to communication[31] , and right to privacy.[32] These fundamental rights protect against excessive government intervention and often intersect with criminal law relating to cyberspace.

Muluki Penal Code, 2074

The Penal Code of Nepal provides that offences committed by carrying or using an electronic device are an aggravating factor in relation to the original offence.[33] The Code prohibits and punishes offences of sexual harassment,[34]

---

[29] *NP CERT*, GOVERNMENT OF NEPAL, MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY, DEPARTMENT OF INFORMATION TECHNOLOGY, (date of visit 05-14-2022), https://doit.gov.np/en/spage/computer-ert.

[30] CONSTITUTION OF NEPAL, 2072, art 17(2) (a).

[31] *Id.* at art 19.

[32] *Supranote* 32, at art 28.

[33] National Criminal Code, 2074, §38.

[34] *Id.* at § 224.

false electronic records,[35] privacy breach,[36] and other acts done with the dishonest intention of causing fear, terror, annoyance, insult, threat,[37] or defamation[38] of another person committed by means of electronic devices. Furthermore, in cases of libel defamation, the Code imposes an additional penalty in the original punishment where such acts of libel were committed by electronic means or other means of mass communication.

Other Laws

Apart from the provision of the Penal Code, other laws and policies dealing with cybercrimes or crimes committed by using electronic devices are listed below. Note that these offenses, though falling within the ambit of cybercrimes, have not been regulated by the ETA, and therefore, they are not considered as pure cybercrimes in the context of Nepali law. They are:

- The Banking Offence and Punishment Act, 2008
- Act Relating to Children, 2075 (2018)
- Some Public (Crime and Punishment) Act, 1970
- The Patent, Design and Trademark Act, 1965
- Copyright Act, 2002
- Consumer Protection Act, 2075 (2018)
- Telecommunications Act, 2053
- National Penal Code, 2074

Finally, the Researchers would like to note that currently, two laws are being discussed in the Parliament that deal with specific issues relating to

[35] *Supranote* 35, at §276.
[36] *Supranote* 35, at §298.
[37] *Supranote* 35, at §300.
[38] *Supranote* 35, at §307.

cybercrimes, namely - i) The Information Technology Bill, 2075, and ii) The Cyber Security and Cyber Crimes Bill, 2077.

Complaint Registration Mechanism

According to Section 75 of the ETA, any case deemed to be an offence under this Act shall be initiated by the Government of Nepal as the plaintiff, and such a case shall be deemed to be included in Schedule 1 of the Government Cases Act, 2049. This means that a first information report (FIR) can be made to any nearby police station regarding offences relating to cybercrimes under the ETA. At present, the powers to register and investigate cybercrime complaints under the ETA can be done at three separate places – 1) the Cyber Crime Bureau,[39] 2) the Metropolitan Police Precinct,[40] or 3) the Crime Investigation Bureau (CIB).[41]

Earlier, the cases regarding cybercrimes in the valley were handled mainly by the Metropolitan Police in Kathmandu, and cases originating outside the valley were under the purview of the CIB, given that the Kathmandu District Court has sole jurisdiction to try cybercrime cases. The Cyber Bureau was established in 2075 BS under the Nepal Police Headquarters to specifically deal with the rising criminal activities and challenges relating to cybercrimes, cyber intelligence, cyber security, and cybercrime investigations. There is no clear demarcation regarding jurisdictional authority and investigative powers of the aforementioned bodies, irrespective of the nature or subject matter of cybercrime; therefore, cases can be registered and investigated by any of the three offices. Complaints under the ETA may even be filed at the nearest police station, which will transfer the case to the Kathmandu Cyber Bureau[42]. Since 2020 Cyber Crime Bureau

[39] Located at Bhotahity, Kathmandu.
[40] Located at Teku, Kathmandu.
[41] Located at Maharajganj, Kathmandu.
[42] National Criminal Procedure Code, 2074, §4 provides that FIR of offences falling under Schedule-1 and Schedule-2 to be made at the nearby police station.

started to receive complaints by email, obviating the need to go to the police station. Cybercrime reports can now be submitted by email to cyberbureau@nepalpolice.gov.np. A copy of a valid identity card, such as citizenship, driving licence, or passport, is required along with the email. The victim can even provide a link to the social media accounts of the offender, as well as other information.

According to data collected from the Kathmandu Metropolitan Police and the Cyber Bureau, the following are the number of cases registered at the respective department offices:

Table 2.1: Data on Complaints Registered under the ETA:[43]

Fiscal Year	District Police Precinct (No. of Complaints)	Cyber Bureau (No. of Complaints)
2067 – 68	2	
2068 – 69	7	
2069 – 70	14	
2070 – 71	35	
2071 – 72	28	
2072 – 73	33	
2073 – 74	25	
2074 – 75	81	
2075 – 76	152	357
2076 – 77	107	2301

[43] Data Collected from Kathmandu Metropolitan Precinct and Cyber Bureau (Data up till 2077.12.31).

Chapter 3

Status and Trends of Cyber Crime Cases in Nepal

Earlier in Chapter 1.3, the Researcher has highlighted the various types of offences that fall under the umbrella of the cybercrime law. These crimes vary from offences against any individual to offences against government, society, or business organizations. Like any other country, Nepal is not free from the threat of cybercrimes. Acts of online defamation, blackmailing, harassment, publication of illegal online materials, unauthorized access to a person's account or company's database, hacking, and online fraud are recurring cybercrimes in Nepal.

The ETA came into force only in the year 2064 BS. It provides that proceedings and adjudication of offences concerning cybercrimes, as referred to in Chapter 9 of the Act, are to be handled by the Information Technology Tribunal,[44] but until such a Tribunal is formed and established, the jurisdiction to hear and adjudicate cybercrime cases shall be with the District Court as designated by the Government of Nepal.[45] As per the notice published by the Government of Nepal in the Nepal gazette dated 2064/12/25, Kathmandu District Court is the sole jurisdictional authority to decide cases under the Electronic Transaction Act at the trial level.

Courts play a crucial role in addressing cybercrimes as they try and decide cases and make precedents that fill the gaps in the law. As a result, cybercrime issues and cases are rising in Nepali soil. Cases regarding cybercrimes under the ETA have arrived in Court after four years since the Act came into existence, i.e., from the fiscal year 2067/68 onwards. The first case to consider for the court under the ETA was the ***GoN on behalf of***

[44] *Supranote* 22, at §60(1).
[45] *Supranote* 22, at §60(5).

Shobha KC vs. Bhoj Raj Lingden,[46] where the accused was charged under Section 47(1) of the ETA for the crimes, such as hacking into the complainant's email, and publishing/distributing obscene pictures of the complainant (victim) through her email address. Since then, there have been altogether 253 cases registered and adjudicated at the Kathmandu District Court. At present, 8 cases have been decided by the Supreme Court of Nepal.[47]

According to the data collected from the Record Section of Kathmandu District Court, the number of cases registered within thirteen years regarding cybercrimes under the ETA is shown in the table below:[48]

Table 3.1: Cases Registered and Adjudicated at Kathmandu District Court

Year	Cases Registered	Cases Adjudicated	Cases Appealed
2064	-	-	-
2065	-	-	-
2066	-	-	-
2067	2	2	1
2068	6	6	2
2069	8	7	4
2070	7	7	4
2071	38	38	27
2072	24	24	12
2073	36	35	16

[46] *GoN on behalf of Shobha KC vs. Bhoj Raj Lingden*, NKP 2067, Decision No. 1430.
[47] Supreme Court Annual Report 2076/77.
[48] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

2074	24	23	5
2075	61	60	16
2076	46	46	6
2077	52[49]	-	-
2078	20[50]	-	-
Total	325	249	93

We can see from the table above that there has been an ever-increasing trend in the number of cases in subsequent years, due to which the Kathmandu District Court has had to deal with such an increasing yearly caseload. Of the total cases registered till 2076, 249 cases have been adjudicated and disposed of, whereas there are still 4 cases pending in court. Further, 93 cases have been considered under the appellate jurisdiction at the Patan High Court.

The ETA does not provide any exhaustive list or definition of the various types of cyber offences. However, from the above observations, the Research tries to classify the various offences falling under the ambit of cybercrime within the Nepali legal structure. These include crimes such as online defamation, harassment, blackmailing, hacking, unauthorized access, data leak, online fraud, etc. The nature and types of cybercrime cases in Nepal are categorized in the table below:

[49] Only data of the registered cases of 2077 were collected, adjudicated and appealed cases statistics could not be collected due to resource constraint.

[50] Data Collected from Record Section of Kathmandu District Court (Date till 2078.02.06). Data files of 2078 were yet to be completely recorded in the Record Section.

Table 3.2: Nature/Types of Cases Filed at the Kathmandu District Court of Nepal[51]

Nature	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	Total
Defamation[52]	1	2	4	4	18	15	15	14	29	19	121
Blackmailing[53]	1	1	2	2	11	11	9	8	20	15	80
Harassment[54]		2	2	2	14	10	12	17	23	20	102
Unauthorized Access[55]				1	1	1		1	2	2	8
Data leakage[56]			1							1	2

[51] Data Collected from Record Section of Kathmandu District Court (Date till 2076.12.31).

[52] Defamation is the wrongful harming of reputation of another by the oral or written communication of a false statement about them. It is the act of defaming another, also known as calumny, vilification, libel, or slander; LeRoy Miller, Roger (2011). *Business Law Today: The Essentials*. United States: South-Western Cengage Learning. pp. 127; Merriam Webster Dictionary

[53] Blackmailing is the extortion or coercion by threats especially of public exposure or criminal prosecution. When cybercriminals infiltrate a private network, grab important data, and hold it hostage, this is known as cyber blackmail or cyber extortion; Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/blackmail .

[54] Harassment is unwanted and unwelcome verbal or physical conduct to create an unpleasant or hostile setting for. Repetitive, unsolicited, hostile behaviour through cyberspace with the goal to fear, intimidate, humiliate, threaten, harass, or stalk someone is termed as cyber harassment; Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/harass .

[55] Unauthorized access refers to approaching, trespassing into, connecting with, storing data in, retrieving data from, or otherwise intercepting and modifying computer resources without consent; https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#:~:text=%22Unauthorized%20access%22%20entails%20approaching%2C,%2C%20systems%2C%20programs%20or%20networks.

[56] Data leakage is the unlawful communication of data from within an organization to an external destination or recipient is known as data leakage. It refers to the unauthorized transmission of data or information from within an organization to a location outside of its secure network.

Hacking[57]					1	1	3			1	6
Fraud[58]						2			1	2	5
Against public morality[59]						1				1	2
Against national Integrity[60]					1						1
Unauthorized Recording[61]					1						1
Data theft[62]			1							1	2
Phishing[63]			1								1

[57] Hacking refers to gain illegal access to (a computer network, system, etc.)[57] Hacking is the unauthorized use of devices such as computers, smartphones, tablets, and networks to harm or destroy systems, collect information on users, steal data and documents, or disrupt data-related activity; Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/hack .

[58] Fraud is a deliberate distortion of the truth in order to persuade someone to part with something of value or relinquish a legal claim. Cyber fraud is a crime done using a computer with the intention of acquiring another person's personal and financial information that is stored online; Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/fraud .

[59] Against public morality cybercrimes are classified as victimless crimes because no specific victim exists, particularly when perpetrated against consenting adults. The values, or 'code of behaviour,' are generally violated in this form of crime.

[60] Against national integrity cybercrimes are those that hamper the national integrity such as corruption. These kinds of crimes are more enhanced in present days with the help of internet and cyber world.

[61] Unauthorized Recording refers to recording done without formal permission or authorization from the owner, operator, manager, or other person in charge.

[62] Data theft is a type of cybercrime in which fraudsters or hackers obtain unauthorized access to confidential and private information that is not meant to be disclosed publicly. It means the theft of information that might be exploited unethically, bringing huge harm.

[63] Phishing is the process of duping internet users into providing private or confidential information that can then be utilized illicitly, for example, through fraudulent email messages or websites.

The table above indicates various types of cybercrime offences reported and tried in the Kathmandu District Court under the ETA. Observing the existing patterns and trends of cybercrime in Nepal, it is visible that the most common forms of cyber offence are those offences relating to online defamation, online harassment, and blackmailing – all of which can be tried under Section 47 of the ETA.[64] Of the total cases registered at the District Court, the majority of the cases are offences involving online defamation, blackmailing, and harassment. In fact, over Ninety percent of the total cases. Other offences under Section 47 include publishing any material against national integrity and public morality or decency.

Table 3.3: Sections Relating to Cybercrime Cases[65]

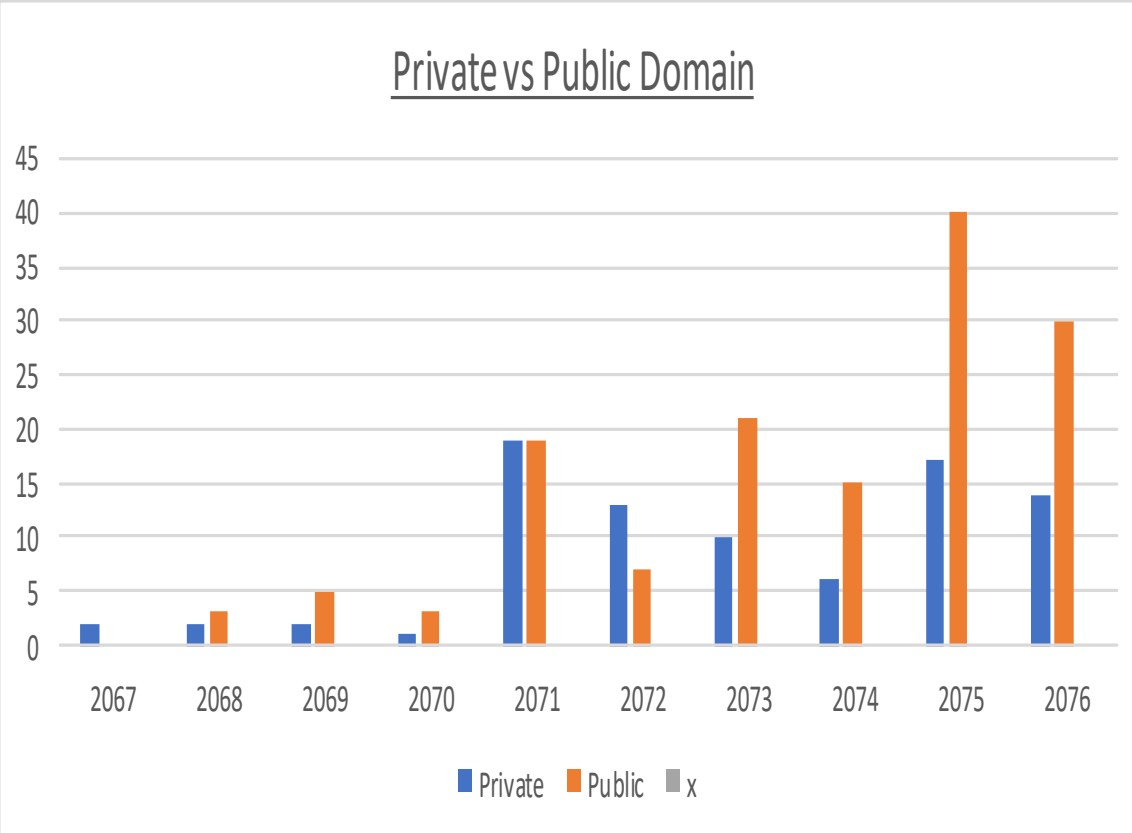
Section	No. of Cases
Sec. 44	2
Sec.45	9
Sec. 46	2
Sec. 47	235
Sec. 52	5

Section 47 of the ETA has criminalized the act of publication of illegal materials in an electronic form, stating that the unlawful content must not be 'published.' To mention here, 235 out of 253 cases registered in the Kathmandu District Court based on the publication. The nature of cases filed is mostly the publication or display of any material via an electronic device or online, either in email, social media, or newspapers, to be regarded as a cybercrime.

However, the term 'published' is open to interpretation since it is not defined in the Act, and neither is it consistently looked into by Courts while analysing the nature of evidence. The question remains - whether published

64 ETA 2008, §47: Publication of illegal content on electronic devices.
65 Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

content must only be in the public domain (Facebook feed, blogs, YouTube, Online News, etc., including group messaging, which has been reachable to public access) or whether it includes content published in the private domain (direct messages, emails) as well. Of the total cases arising out of the publication of illegal content, 86 cases were filed in the court based on content not published in the public domain, and 143 cases were filed in the court based on content published in the public domain.[66]



[66] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31)

Of the cases decided based on the publication of illegal content, there is a 60 to 40 ratio of publication in the public domain versus the private domain. However, there are instances where the court looks into this difference, as data shows that out of the total cases falling under Section 47 which courts dismissed, i.e., around twenty percent of the cases have been dismissed on the grounds of publication of content was only happened in a private domain - targeted in a private forum which can only be accessed by the victim, such as private text messages, WhatsApp, Viber, FB Messenger. As such, the likelihood of punishment in publication cases in the public domain is higher though a clear interpretation of this definition is yet to be made.

Most of the publication-based cases relate to social media offences as it allows the user greater access and availability to harm and hurt the dignity and reputation of another person. It must be noted that most of the social media sites came into existence after the promulgation of the ETA; for example, YouTube was started in 2005, and Facebook was in 2006. Some of the common places for cybercrimes in Nepal include social media platforms like Facebook, Instagram, YouTube, and Tik Tok; Messaging apps like WhatsApp, Viber, Messenger, and Direct Messaging; Emails; Online Gaming Communities; and other forms or chat rooms and news portals. Cybercrime offences such as social media/online harassment and threats, defamation, illegal data access, pornography, phishing, and theft are often found committed through these platforms.

Table 3.4: The platform used for social media (Cyber) Crimes based on the cases registered in the Kathmandu District Court[67]

Online Platform	Total
SMS (Direct Messaging)[68]	36
Facebook	166
Viber	4
E-mail	10
YouTube	5
Twitter	1
Mass media	4
Website	5

Another observation drawn from the analysis of cases shows that out of all the cases relating to the illegal publication of materials made through online harassment, defamation, or blackmail, more than Eighty percent of the crimes are targeted against women – a new trend of gender-based violence against women. Police investigations show that women are targeted online for trolling, bullying, deliberately improper or derogatory comments on their social media posts, using abusive languages online, disclosing personal messages or private pictures, blackmailing, and sexual harassment and objectification. Some men also misuse women's pictures to create new accounts to trick other men – commonly known as catfishing.

[67] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

[68] Although SMS technically does not fall under cybercrime as the definition of cybercrime mentions the use of internet, in context of Nepal, some cases where SMS was used as a medium for committing crimes have also been taken under and dealt as cybercrime.

Table 3.5: Data Relating to the Gender of the Victims[69]

Gender of victims (FY)	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	Total
Female	1	6	6	6	26	14	20	15	47	37	178
Male	1	-	1	-	10	4	12	2	11	5	46

The pattern of cybercrime cases has evolved over the years. In contrast, previously, offences were limited to email & text blackmail and illegal publications online. Still, new types of offences, such as hacking, phishing, fraud, theft, copyright infringements, online, child pornography, deepfake pornography, data theft, etc., have found a common place in cyberspace. Moreover, the increase in the e-commerce business and social media sites and the ease of internet access have led to a greater misuse of cyber platforms, resulting in fewer cybercrimes.

The next most frequently occurring cybercrimes under the ETA include offences under Section 44 and 45 – cases regarding hacking, unauthorized access, data breach, data leakage, and piracy – and cases under Section 52 – cases regarding computer/online fraud. These cases form around Six percent of the total cases tried by courts. As more and more individuals create an online presence and as companies opt for e-commerce platforms to carry out their businesses, their customer data gets collected, which is private data. Recently, cybercrime cases have been filed on behalf of popular businesses like *Foodmandu* and *Vianet Cablenet* for breach of the database through unauthorized access, which is a crime under Sections 45 and 44 of the ETA. Similarly, crimes of online fraud by stealing or diverting money,

[69] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

creating fake profiles/websites or false identity, phishing, ATM thefts, etc., are some of the new areas of cybercrimes.

Table 3.6: Data of cases relating to Section 44, 45, and 52[70]

Issue (FY)	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	Total
Unautho-rized Access				1	1	1		1	2	2	8
Data leak			1							1	2
Hacking					1	1	3			1	6
Fraud						2			1	2	5
Phishing			1								1

The number of cybercrimes has further increased during the COVID-19 pandemic. Due to lockdowns, people were confined within their residences and had more hours and instances of interacting online in their daily lives. While these digital tools have enabled people to work and study from home during the lockdown, they have also exposed people to cybercrime risks. As such, in the fiscal year 2077 itself, over 2,300 (Two Thousand Three Hundred) complaints were filed at the Cyber Bureau, a steady increase from the three hundred complaints filed the previous year. For a worthy mention here, on June 22, 2020, while Nepal Tourism Board was hosting a virtual meeting via the Zoom app, an unknown user hacked into the meeting and

[70] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

played a pornographic video clip just as the Minister was about the address the meeting.[71]

In the last part of this Chapter, the Research shall delve into judicial trends regarding the status of conviction and acquittal upon adjudication of cybercrime cases in Nepal.

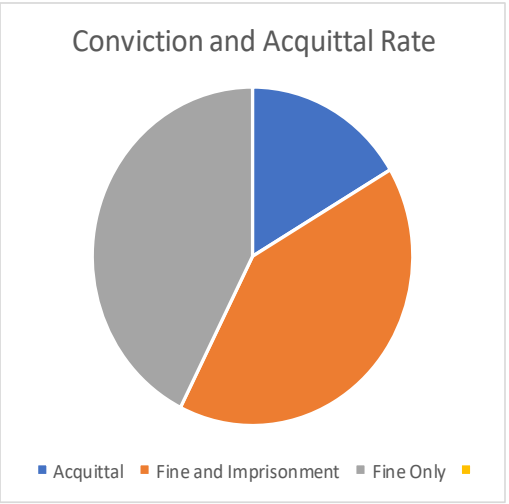
Table 3.7: Status of Conviction and Dismissal of Cases Adjudicated

Year (FY)	Cases Adjudicated	Conviction	Acquittal
2067	2	0	2
2068	6	6	0
2069	8	4	4
2070	7	3	4
2071	38	28	10
2072	24	20	4
2073	36	33	3
2074	21	20	1
2075	61	54	7
2076	46	40	6
Total Cases	**249**	**208**	**41**

Looking into the numbers of conviction and acquittal, we can see a relatively high volume of conviction rate, with 208 out of 249 against the number of acquittals punished either with fine or imprisonment, or both. This denotes around Eighty percent of the cases resulting in the conviction of the

[71] Editorial, *Zoom bombing disrupts Nepal Tourism Board video conference*, THE HIMALAYAN TIMES, (June 2020), https://thehimalayantimes.com/kathmandu/zoom-bombing-disrupts-nepal-toursim-board-video-conference.

accused. This, however, does not tell the entire story since the majority of the cases of conviction have been settled with meagre fines or minimal terms of imprisonment. The reasons for this are dissected in the next chapter, dealing with challenges relating to cybercrime law enforcement.



The data shows that there was no imprisonment imposed on the perpetrator in over Fifty percent of cases (106 cases) of conviction. Rather only they were punished with a fine. Fines are also imposed on the lower side, with some penalties being as low as two hundred rupees. The average fine imposed comes out to be Fifteen to Fifty thousand rupees.[72] The remaining 41 cases resulted from an acquittal as the case could not be proved beyond a reasonable doubt due to many reasons – lack of evidence, inconclusive evidence, ultra vires of the ETA, private domain publication, false prosecution, and so on. The table below provides the information in this regard.

Table 3.8: Term of imprisonment:[73]

Year	No. imprison-ment	Less than 15 days	From 15 days to 1 month	From 1 month to 3 months	From 3 months to 6 months	From 6 months to 1 year	Acquittal
Total	106	22	38	24	11	7	41

[72] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).
[73] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

Table 3.9: Range of fines imposed[74]

Year	No Fine	Up to Rs 15,000	Rs 15,000 to 50,000	Rs 50,000 to 1 lakh	More than 1 lakh
Total (No. of Cases)	17	91	95	4	1

Table 3.10: Range of Compensation granted[75]

Year	No Compensa-tion	Upto Rs 15,000	Above Rs 15,000 - Upto Rs 30,000	Above Rs 30,000- Upto Rs 50,000	Above Rs 50,000 - Upto Rs 1,00,000	More than 1 lakh
Total (No. of Cases)	80	45	35	22	3	1

Thus, from the summary of the findings, it is clear that conviction is largely associated with less stringent sentencing and compensation.

Additionally, the Research has analysed about 80 cases adjudicated by the Kathmandu District Court sampled and selected based on the nature of the offence, uniqueness, modus operandi, popularity, magnitude, and difficulties faced by the courts with their complex nature, and a few cases selected based on random sampling as well. The chart regarding it has been given in Annexure – I.[76]

[74] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).
[75] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).
[76] See Annexure-1.

The IT sector of Nepal is not yet fully developed compared to other developed nations, but the growth and use of the internet, computers, and mobile phones across the country has created the space and opportunity for online criminal acts or using a computer device. Most cybercrimes occur in a few common areas, such as online defamation, harassment, blackmailing, limited instances of hacking and unauthorized access, etc. However, soon, the Government of Nepal will have to prepare itself to deal with various challenges in the cyber space, such as a threat to cyber security and data privacy, malware-ransomware attacks, cyber terrorism, espionage, and deep fake media, and so on.

Chapter 4

Problems and Challenges

The widespread use of computers and the internet has led to the proliferation of various cybercriminal activities, thereby creating new challenges for the criminal justice system to examine and settle cases relating to cybercrimes effectively. The complex nature of cybercrimes makes them different from other conventional crimes, and as such, it requires careful examination with a certain degree of expertise. With its limited resources in terms of manpower, knowledge, and technical knowledge, Nepal is not exempted from the threat of cybercrimes and is witnessing a steady incline in the number of such crimes. It is therefore important to identify and highlight the challenges faced by the criminal justice system at various stages, *i.e.*, from registration of complaints to the investigation, prosecution, and adjudication of cases, so that we may understand the underlying problems existing in the legal regime and, consequently, find solutions that bridge the gap so identified, leading to proper and effective implementation and enforcement of cybercrime laws in Nepal.

For this purpose, the Research has identified key challenges faced by the Kathmandu District Court and the criminal justice system in dealing with cybercrime cases in Nepal. These challenges are experienced in several forms and have been addressed below: -

A. Lacuna in the Legislation

The defective law itself is the foremost difficulty in dealing with cybercrimes in Nepal. Firstly, there is no specific law that deals with cybercrimes in Nepal, as discussed in Chapter 2 of this research. The ETA is the only major law dealing with cybercrime issues, though, in a limited manner. While

looking at the preamble of this Act, it is clear that the law was essentially brought about to regulate the matter concerning digital and electronic signatures. In this Act, only a few sections relating to cybercrimes were inserted under this Act. Thus, the law is now popularly known as the 'Cyber Law of Nepal' though this Act does not substantially deal with cybercrimes.

Under the ETA, only the following crimes have been classified as cybercrimes[77] - to pirate, destroy, or alter computer source code; unauthorized access to computer materials; to damage to any computer and information system; publication of illegal materials in electronic form; to disclose confidentiality; to commit computer fraud; abetment to commit computer-related offence and accomplice of offence.

Further, the language of this Act is vaguely worded, leading to multiplicity in interpretations and creating confusion in existing legislation. It was also noted that the Act fails to address the vast area of cybercrimes. Since its inception, the ETA has seen very little change, while the scope of cybercrimes today is much wider and covers several other issues, such as cyberbullying, identity theft, data interference, deep-fake videos, child pornography, and copyright infringement, phishing, and even cyber terrorism & warfare.

As such, the provisions of this law aren't adequate to tackle cybercrimes increasing day by day. The offences need to be defined clearly. In addition, offences in online defamation, blackmailing, harassment, and phishing are some of the most common types of cases witnessed in Nepal – are not defined anywhere in the ETA. Furthermore, the words used under this Act, such as morality, public decency, publication, etc., have not been defined within the legislation and are prone to rampant misuse.

[77] ETA 2008, Chap 9.

When we look at the data, the maximum number of cases recorded under the ETA fall under defamation and character assassination – which is partly covered by Section 47 of the Act. There is often confusion in Courts as the country already has a separate law dealing with defamation through electronic means. The problem caused by the lack of clarity has created a situation where there is a conflict in domestic laws. The prosecution remains unclear in relation to a charge indicted against the accused. This creates a challenge for the Courts while determining whether or not such offences fall within the ambit of the ETA. Since these are not new crimes but are crimes committed online (where the computer or technology is used as an instrument and not as a target), there is the general confusion and lack of consensus as to which law prevails in dealing with such offences.

Furthermore, some Judges have questioned the idea of prosecuting someone for online defamation under the ETA when there already exist provisions for the same under the Penal Code. The data below shows that around ten percent of cases filed in the court were dismissed because online defamation cases must be tried under specific laws. For instance, in the cases of the Government of Nepal *v. Prakash Dangol*[78] *and the Government of Nepal v. Hari Panta,*[79] the Court dismissed the charge, and the accused were acquitted. The court is of the verdicts that despite a derogatory or libellous content being published online, they are to be tried under the provision of the Penal Code. Similarly, in another case, a person entered the Supreme Court building and recorded conversations with various court officers, and even though there was a crime of illegal recording and breach of privacy, the offence could not be tried under Section 47 of the ETA. The court has decided the case with its verdict.[80]

[78] 071-CR-1166.
[79] 070-CR-0146.
[80] *GoN vs Prabhat Kumar Gupta,* 072-CS-0882.

Similarly, another frequently occurring offence under the ETA is online harassment and cyberbullying, which have been targeted mainly against female victims. This is also an area of conflict in domestic laws. Data shows that over Eighty percent of the cases filed in the Court are pertaining to crimes against women, such as harassment and blackmailing, and causing mental distress to them. However, the Act does not define these terms, and the said offences are tried under Section 47 of the ETA, which relates to the publication of illegal materials. It has also been noted that offences of harassment against women (typically sexual harassment) are dealt with under Section 224 of the Penal Code, 2047, which prohibits sexual harassment through electronic means. There is no clarity as to which statute becomes applicable in such situations. There is a need to address this type of confusion, as this is a modern trend relating to gender-based violence against women.

Further, Section 47 of the ETA states that unlawful content must not be 'published.'[81] Publication is the act of making something generally known. Therefore, the fundamental point of definition is 'published.' A question may arise here whether the term 'published' means to include the material posted in either a private or public domain or only in a public domain. A private domain would be a domain that can be accessed only by the victim and accused and may include their social networks, and a public domain would be a domain that the public at large can access, whosoever may be the one. To illustrate, the lacuna – A and B are in a closed social media group with 50 other people, and A posts unlawful content relating to B on the said closed social media group of 52 people. The confusion that would arise would be whether this is a private domain or a public domain. Thus, the term 'published' not being defined for the said section leaves room for diverse interpretations. For instance, in the cases of the *Government of*

[81] ETA 2008, § 47: Publication of illegal materials in electronic form.

Nepal v. Narayan Paudel,[82] the Government of Nepal *v. Subhash Kumar*,[83] the Government of Nepal *v. Rahul Balmiki*,[84] and the Government of Nepal *v. Biswas Shrestha,*[85] the court gave acquittal to the offender, stating that the material was merely published in the private domain and shared with the masses at large, but in other cases of very similar nature, including the Government of Nepal *v. Tej Raj Joshi*,[86] the Government of Nepal v. *Bikram Malla Thakuri*,[87] the Government of Nepal *v. Sambhu Sunwal*,[88] the Government of Nepal *v. Dhundi Raj Basnet*,[89] The perpetrator was punished even though the content was in the private domain only.

More importantly, crimes of fake profiles/false identities on social media are rising in Nepal. This is an act of representing a person, organization, or company that does not exist. The ETA deals with this in a cursory manner under Section 52, which contains provisions for preventing computer fraud. However, this Section was not drafted to specifically tackle the above-mentioned offences and deal with all forms of computer-related fraud. Without clear definitions of specific offences, there exists ambiguity for the victim (while making complaints), the prosecutors (while establishing the charge), and the Courts (while adjudicating the case).

The vague and ambiguous construction of the Act has also created space for abuse of power, position, and resources by Government officials or business executives who seek to suppress the voice of journalists, writers, artists, and the public criticizing them. A prominent case in relation to this is that of

---

82 073-CR-0395.
83 073-CR-3169.
84 072-CR-0086.
85 22-39-069-2667.
86 Case No. 2750 Year 2068.
87 074-C1-0047.
88 076-C2-0011.
89 074-CR-0895.

journalist Raju Basnet[90] who was harassed with a cybercrime case for writing a report about the connection between political leaders of the ruling party with several land mafia groups. Similarly, in a case of the same type, a young Nepali youtuber named Pranesh Gautam was arrested and kept in custody for six days to review a Nepali movie and present satirical comments about the said movie on his YouTube channel.

The ambiguous nature of the law means that the provisions of ETA can be interpreted in a manner where anything and everything can be considered cybercrimes as long as it is done online via a computer or mobile device. Since cases of cybercrimes are cognizable offences, the accused can be arrested and put in detention for investigative purposes for up to twenty-five days, meaning, irrespective of the fact that the person accused is guilty of the crime not. In other words, the person can be put behind bars, thereby curtaining their personal and civil liberties. Furthermore, there are no provisions in the law regarding compensation for wrongful arrests. Such tactics for suppressing free speech and making a false prosecution threaten democracy. Keeping in view all these, the Kathmandu District Court judges have underscored the need for separate cybercrime legislation in Nepal. They all agree that the present ETA does not cover all aspects of cybercrimes, and thus separate legislation is needed to meet the demands of the modern-day. They suggest that the same can be done by meeting international standards in this regard. They further express an urgent need to establish the Information Technology Tribunal as per the Act. Moreover, many cases have not entered the Supreme Court, and thus, proper precedents through the right interpretation are yet to be given. Without clear precedents, the vague and ambiguous construction of the Act has created hindrances in dealing with such offences by Courts.

[90] Editorial, *Journalist arrested for online news story*, MY REPUBLICA (September, 2019), https://myrepublica.nagariknetwork.com/news/journalist-arrested-for-online-news-story/ .

B. Lack of Investigative Tools relating to Nature of Evidence

The fight against cybercrimes requires adequate substantive criminal legal provisions and effective procedural rules to carry out effective investigations. But unfortunately, there are no separate procedural handbooks, manuals, procedural guidelines, or rules in place with respect to the investigation and prosecution of cybercrime cases in Nepal, and only the general laws of Muluki Penal Code *2074* can be applied to gather, preserve, and present evidence in the court.[91]

From the data collected and analysed in this research, it is found that out of the cases dismissed and acquitted based on the nature of the evidence or lack of it, around twenty-five percent of the accused were acquitted due to lack of evidence.[92] A public prosecutor working in the District Attorney Office, Kathmandu, mentioned that the lack of evidence is one of the major reasons for the failure of the prosecution to establish charges against the offender in court. According to the prosecutor's statement, "*the nature of evidence in cybercrimes is different from evidence in other crimes, and to establish a guilty verdict, a very specific set of evidence is required. But due to the lack of proper investigative tools or outright lacklustre investigation, it is difficult for the prosecution to prove the case and for the court to render a guilty verdict in these cases*."

An important factor that makes cybercrimes more difficult to investigate and prosecute compared to other traditional crimes is the nature of the evidence. The value of evidence is paramount, and this is true, especially under criminal law, since these cases need to be proven beyond a reasonable doubt. Unlike other crimes where physical evidence is available, it is not so possible in cybercrime. The evidence of cybercrime is mostly found in data that must be tracked or traced with the help of computer networks or the

[91] National Criminal Procedural Code, 2074 §8 deals with Collection of Evidence.
[92] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

internet. Further, without guidelines for handling digital evidence, where the proper chain of custody is not maintained, such evidence can easily be questioned in court as to its inadmissibility. The problem is further compounded by the fact that without any legal guidelines, ISP companies in Nepal are only bound to hold data/information of their users for up to six months in their database, meaning investigation must be done promptly. The statutory limitation to file a case in the court is only thirty-five days, which may be deemed too short from the perspective of investigating agencies.

To test digital data or electronic evidence, the original device (mobile phone, laptop, computer, etc.) is necessary for proper investigation. Whereas under the ETA, complaints are made based on online links or photocopies of published content, and there are no provisions regarding – a) production of computer systems & data and b) search, seizure, preservation, and presentation of digital evidence. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. However, in the absence of proper procedural guidelines/ manuals/rules/laws on identifying, collecting, preserving, and presenting digital evidence, effective prosecution and adjudication of cybercrime cases are beyond the expected outcomes.

A present, two separate forensic kit labs have been set up at the Cyber Bureau (in 2075) and the Nepal Police Headquarters (in 2073) to provide digital forensic investigation services in Nepal. According to the police sources, the labs were designed using the latest tools and computer software and hardware, with specialized police personnel and technical experts to process and investigate digital evidence. Moreover, the National Computer Emergency Response Team, 2075 was created to perform forensic investigation and analysis of cyber incidents, responding to cyber security

incidents, and coordinating with global and local agencies and organizations towards combating cybercrime case.

However, the reality is that despite their best efforts, sometimes due to the insufficient legal tools or expert personnel to collect and handle evidence and conduct proper investigation, forensic investigation in cybercrime cases becomes difficult to tackle. Furthermore, even when a proper investigation is done by the cyber security personnel, there are other challenges like presentation of the evidence in court during prosecution. Due to inadequate IT infrastructure and dedicated technicians in the courtroom along with budgetary constraints and other problems as highlighted in this chapter, presenting of evidence by the forensic expert or security personnel is not as clear or cohesive as it should otherwise be which may lead to misinformed adjudication of certain cases.

C. Centralized Jurisdiction of Court and No Proper Capacity-Building

The ETA provides for an Information Tribunal, which shall be the court of the first instance in relation to cybercrime cases.[93] It further states that one of the members of the said Tribunal must come from the technical field. This shows that the legislature is cognizant of – a) the need for a separate court that exclusively deals with cybercrime cases and b) the need for an adjudicating authority that has proven technical knowledge in the concerned field. However, even after 15 years of the promulgation of the ETA, such a Tribunal is yet to be established. Therefore, in lieu of such a Tribunal, all cybercrime cases in Nepal are being prosecuted at the Kathmandu District Court. The experience of the Kathmandu District Court in this regard thus becomes valuable while assessing the shortcomings of a centralised and under-capacitated justice delivery system pertaining to cybercrime cases in Nepal.

[93] ETA 2008, §60(1).

A centralized jurisdiction for cybercrime cases means that regardless of where the crime originates, it will come under the jurisdiction of the centralized court, at present, the Kathmandu District Court. This results in limiting access to justice and overburdening the court's business. Restricting the access to justice happens when complainants find it difficult to travel from across the country to reach the centralised location throughout the hearing, as it adds to the cost of pursuing the litigation. The Kathmandu District Court has witnessed an overburdening of cases. As a result, nationwide cybercrime cases are being added to its pre-existing docket. At present, the Court hears Cybercrime cases and adjudicates all other civil and criminal cases that were already under its jurisdiction, thereby leading to an over-burdening of the Court and adding to the pendency of cases.

It has also been noted that, since cybercrime is a very technical area of criminology, the judges also need to be well-versed in this field by way of proven experience and/or training. Judges at the Kathmandu District Courts are generalists in nature, whereas the issue of cybercrime requires a specialist's attention with some degree of knowledge and expertise. However, there are only a handful of judges in Nepal who have some experience and background in the field of cybercrimes. Moreover, when cases are distributed evenly and randomly to all judges, one Judge presides over one to two cybercrime cases each year. This does not allow them to grasp and comprehend the subject matter thoroughly instead, unlike other traditional types of cases.

In the interviews with the Kathmandu District Court judges, it was noted that the lack of training in this area is a major hurdle in the proper adjudication of cyber cases. It has been reported that the training of judges for cybercrime cases is non-existent. In the same way, one of the judges stated that due to t lack of training, it becomes very difficult for judges to

ascertain the meaning and value of the evidence. Therefore, the Information Tribunal must have a member with technical knowledge who should solve this problem when the said Tribunal is established. However, it is strongly recommended that until the jurisdiction of cybercrime cases remains with the Kathmandu District Court, the concerned judges handling cybercrime cases need to be given technical training.

Further, due to the lack of adequate training and education of judges in cyber law, and the over-burdening of courts, the time taken for case disposal is lengthy and cumbersome. For example, the table below illustrates that the average time taken to prosecute and adjudicate a case, *i.e.*, from registration in court to passing of verdict, takes up to 6 months. Some cases even take over a few years at trial.

Table 4.1: The speed at which cases are decided[94]

Year/ Duration	Upto 1 month	More than 1 month- Upto 3 months	More than 3 months- Upto 6 months	More than 6 months- Upto 1 year	More than 1 year - Upto 2 years	More than 2 years	Total cases in a year
Total	18	53	85	59	23	3	245

The Supreme Court of Nepal, in the case of *Advocate Rajaram Shrestha v. The Government of Nepal,*[95] has already ordered the Government of Nepal to establish the IT Tribunal. However, the government is yet to enforce the statutory provision and execute the judicial decision. However, merely establishing an IT Tribunal may not solve all the problems in prosecuting and adjudicating cybercrime cases. This Tribunal is likely to face the same

[94] Data Collected from Kathmandu District Court Records Department (Data up till 2076.12.31).

[95] *Advocate Rajaram Shrestha v. Nepal Government,* Writ Number 067-WO-0524.

issues being faced by the Kathmandu District Court, such as overburdening of cases and limited access to justice due to the continued centralized jurisdiction of the Tribunal.

D. Jurisdictional Challenges

Another issue to deal with is jurisdictional challenges. Cybercrime is a transboundary crime where a cyber-attack can originate in one country but impact another country. The issue of jurisdiction is fundamental to all legal systems worldwide, as Nepal has been facing nowadays. One of the major issues regarding jurisdiction is that courts generally do not have jurisdiction beyond their boundaries. In that event, the only way to get the accused/perpetrator to Nepal is through extradition, which comes with its complex challenges.

In cybercrime cases, without identifying the perpetrator first, the case does not proceed. When a crime originates from abroad, the task of identification becomes especially hard. Furthermore, gathering data and evidence requires coordination with offices from foreign countries. For example, suppose a crime of online defamation was carried out via Facebook. In that case, the police must wait to verify content from Facebook Headquarters located in the United States as there is no Facebook office in Nepal. The same goes for other social media sites such as Instagram, YouTube, or Tiktok. Moreover, in many countries, crimes relating to social media offences are not under the mandate of cybercrimes, and thus these companies are hesitant to release the data with urgency. Differences in language, culture, attitude and perception of different countries regarding what constitutes cybercrimes are hindrances to effective investigations.

The challenges relating to investigating cybercrimes affecting Nepal but originating aboard get further aggravated as Nepal is not a part of the Budapest Convention or any other International Treaties relating to

cybercrimes. For example, during the lockdown due to Covid-19 in 2020, several complaints were filed regarding deep fake pornographic videos targeting Nepali actresses and celebrities circulated online; however, it was found that the videos originated from India and other foreign jurisdictions. Therefore, the perpetrator could not be identified, and no action was taken as the case could not be pursued further. As such, jurisdictional challenges extend to identifying perpetrators outside of Nepal, tracking and tracing the IP address, and further barriers of language, culture, and attitude. The solution to these jurisdictional challenges lies in international cooperation alone. Thus, Nepal should endeavour to become a signatory of the Budapest Convention and other international treaties that deal with cross-border cybercrimes.

E. Enforcement Challenges

While examining the challenges relating to trends of the judiciary in the adjudication of cybercrime cases, enforcement of punishments in cybercrime cases has also been identified as a major weak spot. On the one hand, the cyber law in Nepal seems harshly punitive as most of the accused are convicted, even when the nature of the crime itself is not that serious. Similarly, not enough penalty is imposed on the guilty person, as most are let go with meagre fines and minimum sentencing. It has been observed that there is no uniformity in sentencing in the trial court. Due to a lack of laws and a lack of proper understanding of the subject matter of cybercrimes, imprisonment or fines – including compensation – are generally imposed on the lower side. As discussed earlier, the maximum punishment for the person convicted of cybercrime in Nepal is three years, with the exception of Section 47, where punishment is up to five years. However, the sentence imposed is between fifteen days to one month, whereas the fine imposed is between fifteen to fifty thousand rupees. In many cases, judges simply

impose minimum punishment because they are under pressure to punish due to the possibility of backlash from media or law practitioners.

The data shows that in over fifty percent of cases of punishment, there was no imprisonment imposed against the perpetrators. They were punished with a minimum fine. The table below provides the information.

Table 4.2: Term of Imprisonment

Year	No imprison-ment	Up to 15 days	More than 15 days Up to 1 month	More than 1 month-up to 3 months	More than 3 months to 6 months	More than 6 months up to 1 year	Acquittal
Total	96	14	34	21	10	6	41

Table 4.3: Range of Fines Imposed

Year	No Fine	Upto Rs 15,000	More than Rs. 15,000 to less than Rs. 50,000	More Rs. 50,000 to less than 1 lakh	More than 1 lakh
Total	11	81	93	4	1

Table 4.4: Range of Compensation Granted

Year	No Compensa-tion	Upto Rs 15,000	Above Rs 15,000 - Upto Rs 30,000	Above Rs 30,000- Upto Rs 50,000	Above Rs 50,000 - Upto Rs 1,00,000	More than 1 lakh
Total	80	45	35	22	3	1

Due to the punishment being meted out in minimum quantum and the comfortable expectation of being released on bail with a minimum amount, there is a lack of deterrence to hold the criminals from committing cybercrime offences. Therefore, until or unless the challenges laid down in

this research are properly dealt with, the challenges to enforcement of cybercrime cases will continue to persist.

F. Additional Challenges

In addition to the challenges faced in the criminal justice system, cybercrime victims have to deal with hurdles while filing FIRs. As mentioned earlier, jurisdiction in relation to complaint filing is given to the Metropolitan Police, the Cyber Bureau, and the CIB. However, the lack of clear distinction sometimes creates confusion about where such cases are to be filed and who has the final jurisdiction to record and investigate such cases. For instance, in a cybercrime case against a foreign national woman in Nepal, she was incessantly harassed online with several false and baseless materials published via Facebook and other online news portals. When the complaint was first made at the Metropolitan Police, Teku, she was told to go to the Cyber Bureau. However, the Bureau did not entertain and register her case as they claimed that the case falls under the purview of defamation and must therefore be filed directly at the Kathmandu District Court instead. Cases of similar nature or even of lesser degree have been allowed under ETA by the police. This arbitrary setup has led to doubts in the minds of people over whether the ETA is simply used as a tool by the police to control cyberspace or exists to give some protection to people against cybercrimes.

Even if a case gets registered with the police, not all cases see the light of day. Last year, there were over 2301 complaints filed at the Cyber Bureau alone. However, only 57 cases were registered in the Court. Similarly, in the year before that, there were 357 complaints filed, of which 52 cases were registered in the Court. This is because not all the complaints filed merit the charge of a cybercrime offence. Since the general public understands that all offences originating online or through the computer system are cybercrimes, several unrelated or unnecessary complaints are made.

Furthermore, unlike other criminal cases, an FIR is not directly lodged in cybercrime cases. Instead, first, a simple application is made, after which the police commence its preliminary investigation. Then, the formal complaint is made once an accused is identified. As such, lack of users' awareness and education; a lack of clear demarcation in relation to the investigative authority; difficulties in identifying and locating the perpetrator; along with the discretionary powers of the investigative authorities to determine what is and what is not a cybercrime offence leaves the door open for errors and misuse of the ETA, especially considering the weak and insufficient legal and regulatory mechanisms.

Chapter 5

Recommendations – The Way Forward

This research holds that identifying any problem is a stepping stone to addressing the identified problems. The research has thus l put into a clearer way the challenges faced by Nepal's criminal justice system (police, prosecutors, courts) with respect to cybercrime enforcement with better understanding. Therefore, in this final chapter, the Research has outlined some recommendations/suggestions to help resolve the existing problems and challenges.

Clear and Cohesive Legal Structure – Eliminate Ambiguity in Law

According to noted jurist Lon Fuller, all purported legal rules must contain eight minimal standards[96] - The rules must be (1) sufficiently general, (2) publicly promulgated, (3) prospective, (4) clear and intelligible, (5) free of contradictions, (6) relatively constant, (7) possible to obey, and (8) administered in a way that does not wildly diverge from their obvious or apparent meaning. Effective prosecution and adjudication of cases require clear and cohesive laws, i.e., rules must be expressed in understandable terms, with as little room as possible for ambiguity or uncertainty. To solve the challenges faced due to the ambiguous and vague construction of the ETA, the first and foremost offences deemed to be cybercrimes must be properly laid down and defined in law. As such, the offences provided under Chapter 9 of the ETA need a clear definition with necessary explanations so that there will not be room for misinterpretation or misuse of the law; thereby, law enforcement becomes consistent and harmonious.

[96] Lon Fuller, *The Internal Morality of Law* (1964).

The frequently occurring types of cybercrimes fall under Section 47 of ETA, relating to the publication of illegal content. This Section needs to be broken down and explained in a manner where people understand what constitutes the term 'publication', whether such publication must be made in the public domain, and the effects and implications of such publication, *i.e.*, whether the publication results in defamation, blackmailing, harassment, social media crimes, or any other offence. The Supreme Court of Nepal, in the case of the Government of Nepal *v. Hari Panta,*[97] has already interpreted the term 'publication' in such a manner that private conversations done through an electronic medium are not deemed to be a publication and therefore denied personal conversations as 'publication' resulting in defamation or insult or reputation in the context of Section 47 of the ETA. Therefore, it is important that this judgement is disseminated amongst lawyers and judges and enforced this case law in lower courts to eliminate the confusion regarding publications of illegal content online. This Section, however, needs further explanations to combat private domain publications causing blackmailing, threats, or harassment to any individual.

Concerning the vague construction of the Act and its potential scope for mischief and misuse, the language of Section 47 under ETA is very similar to Section 66A of the Information Technology Act of India in the sense that it is vaguely drafted, and the very liberal interpretation allowed seems ultra vires to the Constitution, especially the right to freedom of speech and communication. Section 66A of the Information Technology Act, 2000 A.D made it a punishable offence for any person to send 'grossly offensive' or 'menacing' information using a computer resource or communication device.[98] The provision also made it punishable to persistently send information that the sender knows to be false for annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or

[97] Supreme Court, 070-CR-0146.
[98] Indian IT ACT, 1996, §66A.

ill desire. Although it is intended to create a safe environment for internet users, the vague and arbitrary terms used in the Section led to much misuse in various ways, with several criminal cases being instituted against innocuous instances of online speech, including political commentary and humour. Section 66A has been struck down by the Indian Supreme Court for this very reason in the case of *Shreya Singhal vs. Union of India*[99] in 2015 A.D. For the same reason, Nepal should also consider repealing or, at the very least, modifying the language of Section 47 of the ETA.

Furthermore, the meaning and scope of the other offences and the nature of such offences under the Act need refinement and explanations so that crimes relating to piracy, hacking, unauthorized access, and fraud can be included. For instance, under Section 44 of the ETA, the scope of piracy must be expanded beyond computer source code and extend to other forms of computer and information systems, such as data, electromagnetic devices, and computer networks, and should also include digital art, movies, and photograph piracy. Similarly, under Section 52 of the ETA, committing computer fraud must clearly mention whether offences relating to fake profiles, false identity, phishing, and other online theft and frauds are included under this law. Moreover, since most of the cybercrime offences committed in Nepal are technology/computer-related crimes, such crimes can be tried under traditional criminal laws such as harassment, defamation, theft, fraud, blackmailing, etc. This creates a situation wherein law practitioners and courts are unsure whether certain offences committed online are to be tried and punished as cybercrimes under the ETA or relevant criminal law provisions. One in every ten cases of acquittal (ten percent) was dismissed on the ground that the charges were misconstrued, and the case should have instead been tried under specific laws governing the offence. To avoid the ambiguity arising out of the conflict of domestic

[99] AIR 2015 SC 1523, Supreme Court of India.

laws, through judicial or legislative intervention, the existing laws must be interpreted in such a manner that laws are unambiguous, leaving no room for doubts and uncertainty regarding applicable laws in tackling respective offences.

In some ways, the cyber law in Nepal seems harshly punitive even when the nature of the crime itself is not that serious, while at the same time, several cases are dismissed with no or minimum quantum of punishments. According to esteemed cybercrime lawyer Mr. Baburam Aryal, *in addition to amending the law by defining and broadening the scope of certain Sections, it is also important to classify various offences under the ETA into different punitive regimes.* To consider all crimes under the ETA, they must be proved beyond a reasonable doubt; i*nstead of categorizing all crimes under ETA to be deemed as schedule-1 offences, the Act should be amended to classify these offences based on the nature and gravity of offence into - i) civil offences; ii) crime against the state; iii) and a crime against an individual; and proceed accordingly.* This classification of offences seems to deter the scope for misuse of cyberspace and the law while at the same time making adjudication easier and also lessening the burden on a single court by reducing the caseload of the Kathmandu District Court.

Specific Laws to Combat Cyber Crimes

In addition to the offences listed in Chapter 9 of the ETA, new laws must be created, or existing laws must be amended to include other offences or prospective crimes that are not presently dealt with by the ETA. The existing law is almost 15 years old, and since then, there has been substantive development and changes in the information and technological sector. Most social media sites, including Facebook, YouTube, and Tiktok, were born only after the Act came into existence. Any shortcomings in the present law must be addressed by amending the existing provisions as well as adding new laws to incorporate other offences pertaining to cybercrimes such as

cyberstalking; cyberbullying; sexting, pharming, malware/virus/Trojan threats and attacks, illegal interception of communications; commercial/corporate espionage; dissemination of fake news; cyber terrorism and warfare; online money laundering, gambling, or prostitution; child pornography and deep fake videos amongst others.

With the need for a specific special law to deal with the rising trends of cybercrime cases, the Information Technology Bill (hereinafter called IT Bill) was drafted, which is presently being discussed in the Parliament, making forward steps to include far-reaching aspects of cybercrimes not included in the ETA. The IT Bill is being developed to replace the existing Electronic Transaction Act and is touted by the government as the most comprehensive and clear law to address the long-held concerns around IT management. This Bill aims to bring domestic laws into line with international standards by covering the development, promotion, and regulation of information technology, recognition of digital/electronic records and signatures, cyber security, control of cybercrimes, etc.[100] This Bill deals with twenty-eight different offences falling under cybercrimes, such as cyberbullying, cyber terrorism, sexual harassment, and publication of vulgar/obscene content. As the name suggests, the Cyber Crimes Bill is drafted to deal with specific issues relating to cybercrime offences. It proposes a range of substantial and procedural law provisions to govern cybercrimes.

However, rather than looking for single umbrella legislation to cover everything related to cyberspace in one place, the Government should seriously think about bringing different legislation to address different areas of cyberspace, such as digital copyright, which is to be looked into by the Copyright Act; domain parking, cyber-squatting, and trademark issues to be looked into by Patents Trademarks and Design Act; online sexual harassment and privacy infringement by the Sexual Harassment Act and

[100] Information Technology Circular, 2075, preface.

Privacy Act respectively; and new statues to deal with issues pertaining to cyber security, social media-related offences, cyberstalking, data theft, etc. so that there could not be confusion and conflict between different laws, thereby creating an effective and cohesive cyber law regime. This will further allow charges and punishments to be determined by the offense's nature, modus operandi, and gravity. This idea of separate laws for separate cybercrimes is practiced and prevalent in the United States, with different state and federal laws to govern the different aspects of cybercrimes.

Ratify the Budapest Convention

As the ETA covers Cybercrimes in a cursory manner, there is a necessity for specific laws to deal with Cybercrimes in-depth without creating a conflict in domestic laws. To fill the gaps in the existing law, Nepal should endeavour to become a party to the Budapest Convention as the Treaty addresses internet and computer crimes by harmonizing national laws, providing exhaustive substantial and procedural laws, improving investigative techniques, and increasing cooperation among nations as cybercrime cases often occur in the transboundary sphere. Accession to the Budapest Convention is not itself enough to tackle cybercrimes, and it does not guarantee that all our cyber challenges will be solved overnight. It does, however, provide a platform to build synergies, cooperate with member countries, and ensure commitment to offering stronger resistance to cybercrimes. It has substantive and procedural law provisions relating to illegal access, interception, data interference, misuse of devices, computer-related forgery and fraud, child pornography offences, copyright infringement, and many others. In the context of Nepal, ETA governs cybercrimes issues, and unfortunately, the ETA itself has not defined cybercrimes so that we can understand our level in the context of cybercrime laws. Thus, ratifying Budapest Convention might provide a great

basis and framework for Nepal to form its specific laws dealing with cybercrimes.

In 2018 A.D, the former Attorney General of Nepal recognized the need to draft a cybercrime legislation that incorporates the best practices and fundamental aspects of the Budapest Convention on Cybercrime. Therefore, this can be considered a practical starting point in this regard.

Decentralized Jurisdiction and Capacity Building of Courts

Another major problem identified during this research is regarding the issue of centralized jurisdiction of the Kathmandu District Court and the lack of human resource capacity or necessary skill and knowledge of the judges to handle the cybercrime cases adequately. Therefore, it is of paramount importance to establish the Information Technology Tribunal as envisaged by the ETA itself, as it provides for a three-member tribunal consisting of one member from the field of law, Information Technology, and Commerce. This allows specialization in the subject matter of the Tribunal to handle proceedings and adjudicate cases with a certain degree of expertise. The Supreme Court of Nepal, in the case of *Advocate Rajaram Shrestha v. The Government of Nepal,*[101] has already ordered the Government to establish the IT Tribunal. However, as discussed in the above Chapter, merely establishing the Information Technology Tribunal may not solve all the problems in prosecuting and adjudicating cybercrime cases. This Tribunal is likely to face the same issues being faced by the Kathmandu District Court, such as overburden of cases and limited access to justice due to the continued centralized jurisdiction of the Tribunal. The solution for this challenge is to establish Regional Benches of the Centralized Tribunal, which will function as the Principal Bench, acting as the administrative headquarters while also trying cases within its specified jurisdiction.

---

[101] *Advocate Rajaram Shrestha v. Nepal Government*, Writ Number 067-WO-0524.

In the interim, until such Tribunals are established, the power to try cybercrime cases remains in the hands of the Kathmandu District Court Judges. It is, therefore, very important to prioritize and provide basic training to all judges of the Kathmandu District Court, especially with regard to digital evidentiary value and validity of evidence. Another way to ease the burden of this Court is to assign cybercrime cases to those judges with technical expertise and knowledge in the concerned subject matter. And in the event of a judge transfer, they are to be placed in the Kathmandu District Court. In an interview with Honourable Judge Shri Krishna Bhattarai, assigning cybercrime cases to a small group of judges will allow familiarity to breed in and learn about the nuances of cybercrime issues, making them experts in this area. For instance, cases relating to offences against children are always assigned to the Chief Judge of the respective District Courts.

During the trial, the prosecution and expert witnesses should cooperate to have a due resolution of cases. The courtrooms must be properly equipped with projectors, monitors, computers, and other facilities to present digital evidence. Judges could even consider introducing mixed-system trial procedures (inquisitorial and adversarial systems combined), *i.e.*, enabling the judge to see the evidence before trial because of highly technical and voluminous pieces of evidence presented in cybercrime cases. Moreover, with the introduction of virtual hearings in Nepali courts due to the lockdown due to Covid-19, the Kathmandu District Court should try and continue hearing cybercrime cases in this manner. Since online crimes may be committed from any part of the country and considering the logistical hassles, including time taken, cost, and effort in bringing the accused person to Kathmandu District Court, it could simply carry on with virtual hearing from the districts in which an accused was arrested. The offence of cybercrime itself has the word 'Cyber' in its name. The court could also

introduce in-camera hearings in cases relating to the publication of obscene/vulgar photos or videos online to protect the identity and dignity of the victim.

Expedited and Effective Investigative Mechanism

To improve investigative deficiencies, police officers and investigators should maintain a high level of competency through regular training to ensure the correct handling and examination of digital evidence. In addition, the government should ensure that only specialized and competent officers are allowed to handle cybercrime investigations and establish forensic laboratories equipped with adequate and updated forensic tools, with on-call and available cybercrime experts. The levels of the existing cyber forensic labs must also be upgraded for better cybersecurity risk identification, impact mitigation, and emergency response to make security faster and more secure including several other prospective cyber threats we may be facing in the future. Procedural laws, which specifically treat digital evidence, *i.e.*, translating digital evidence to physical evidence, should be legislated. In this regard, the government must frame digital forensic handbooks, guidelines, and manuals for search, seizure, investigation, preservation, and presentation of digital evidence, so that the proper procedure for looking into digital evidence. Finally, an additional budget must be allotted for cyber security and cybercrime investigations.

Considering the nature of evidence and the various investigative challenges, the cyber bureau has recommended the statute of limitation be extended to a longer period of at least ninety days, if not longer since thirty-five days is too short from the investigative perspective since the investigation of cybercrime cases may take longer than regular crimes. This should, however, be taken with caution and treated carefully, as the very nature of the evidence is sensitive and thus may get lost, destroyed, or deleted at any point without any trace. Hence, extending the limitation period means

maximizing the risk of the availability of evidence whereby the perpetrator can be identified, leaving no legal remedy available to the victims.

International Cooperation

International cooperation plays a vital role in expediting the identification, search, seizure, and preservation of digital evidence since cybercrime is borderless transnational crime to mitigate the jurisdictional challenges. Government should provide a conducive environment for international cooperation, cooperation between agencies, and social media. Procedures for processing requests should be simplified and streamlined, with an adequate capacity for investigating agencies. In addition to ratifying the Budapest Convention, other regional and international treaties, including mutual legal assistance with other countries, must be signed to enhance effective investigation and prosecution of international cybercrimes. As such, international cooperation is crucial in patrolling, reporting, and investigating incidents of cybercrimes and strengthening the cyber agencies.

Victim Protection and User Awareness

Additional safeguards must be put in place by the government to ensure the protection of the online community and raise awareness of the internet users regarding the threats to their identity and assets. Furthermore, core rules of ethics and etiquette in the virtual environment should be communicated to all users. This must be further aided by awareness programs about the rights of the affected party and the legal remedies available to them. Any information provided by the victim must be kept confidential. This requires the support and cooperation from the investigative agencies (complaint registration authorities) in communicating the manner and place to file complaints, with clearly defined jurisdiction of each agency if any. The establishment of the Cyber Bureau in 2075 B.S is seen as a positive step to improve the deficiencies in the complaint

registration mechanism. More recently, the Bureau has even facilitated complaint applications online via email. This is a good step towards victim protection as the online complaint system is more secure and confidential, making victims' data less likely to be misused. But as mentioned above, the major requirement is user awareness regarding the risks, remedies, and processes.

Conclusion

Cybercrime is an ongoing threat, and it continues to evolve, with new threats and challenges surfacing and its numbers increasing every year. With the technology industry booming, millions of people in Nepal now have access to mobiles phones and computers and internet. Moreover, the Covid-19 pandemic simply led to many people spending more time in front of screen – mobiles, laptops, iPad, computers, etc. – broadening their digital footprint as social media has become central to people's everyday lives and perhaps increasing their overall vulnerability to cyber-attacks and online crimes in the process. These developments have presented serious challenges in law and in the criminal justice enforcement as we struggle to adapt to crimes that no longer occur in the terrestrial world but the virtual environment of cyberspace.

With no specific laws made to regulate, restrict, and enforce online activities and cybercrimes in Nepal, the existing legal mechanisms to combat cybercrimes are weak and incohesive. Nepal at present, relies on the Electronic Transaction Act (ETA), 2063 to regulate and control offences relating to computer and computer system, as deemed to be cybercrimes. This law is over 15 years old in dire need of revamping as there has been substantial developments and changes in the field of modern technology – most social media and online platforms widely used today were created in the last fifteen years or so. With provisions relating to piracy, hacking, unauthorized access, illegal publication online, and computer fraud, the ETA acknowledges certain cyber threats albeit in a limited manner only. However, the language in the law is vaguely drafted leading to ambiguity in interpretation and enforcement of law. This has created several challenges to the disposal of cybercrime cases as the lack of coherent and cogent laws results in inconsistent and no uniformity in proceedings and adjudication. It is therefore of utmost importance to eliminate any confusion and ambiguity

– ambiguity in language and ambiguity in cases of conflict of law – to better manage cybercrime cases in Nepal.

Existing laws need to be revised and new laws must be made not only to cure the ambiguity in the existing legislation but also to include prospective cybercrimes that are not presently contemplated in law. The rise in online and technology based criminal activities like cyber terrorism and warfare, ransomware, viruses and trojan attacks, cyber bullying and stalking, child pornography and child grooming, fishing, online fraud, identity theft, data breach, cyber-squatting, and many more, the prevailing laws on cybercrimes, or more precisely the lack of it, must be addressed by amending the existing provisions but also by creating new laws to specifically deal with the rising cybercrime cases. The introduction of the ICT Policy, 2072 and CERT Guidelines, 2075, as well as the proposed draft IT Bill and CC Bill, itself acknowledges the fact that there is a need for revision of the existing cybercrime laws.

At present, all cases pertaining to cybercrimes in Nepal are tried at the Kathmandu District Court. Cases mostly range from illegal publications online (section 47 of ETA) – online defamation, harassment, threats, blackmails, against public/national morality, posting vulgar photos, etc., to other activities like online fraud, false identity, data breach, hacking and unauthorized access. It is important to note that a vast majority of cybercrime cases in Nepal are committed against women thus highlighting the need for safe space for women online. Despite the best efforts of the Kathmandu District court, its centralized jurisdiction means all such cases nationwide are being tried in a single court thus limiting access to justice and overburdening the Court. This issue is further compounded by the limited knowledge and technical expertise amongst the judges and court officers around cybercrime laws. All these factors contribute towards slow and ineffective conclusion of cases with decisions that are not uniform and

consistently coherent. Therefore, as mandated by the Supreme Court of Nepal's order, the Government must take steps to form the IT (Information Technology) Tribunal as this would allow specialized personnel in the subject matter and a separate legal (judicial) authority to effectively try all matters relating cybercrime cases in Nepal.

Further improvements must also be made to better facilitate and expedite investigative and judicial proceedings. Increasing knowledge and capacity of judges, lawyers, and police through trainings, advanced digital forensics, adequate infrastructures, proper procedures for collecting and handling of evidence, are some of the areas that require immediate impact. The unique and sensitive nature of evidence in cybercrime cases is such that its search, seizure, and examination by an investigator who is not familiar with such subject-matter, more often leads to an inefficient investigation. Therefore, calling upon cyber forensic experts to collect and present digital evidence remains imperative. To have a set of handbooks, guidelines, rules, and laws in this regard is thus a dire need in this area. Furthermore, there is also a need for dedicated technical, physical infrastructural facilities in the form of digital forensic laboratories that assist in collecting and presenting digital evidence.

Thus, in analysing the status and trends of cybercrime cases in Nepal, and in identifying the key challenges to effective enforcement of cybercrime cases, it is without any doubt that the risk of cybercrime poses far more questions than we have the answer to. With ever increasing cases, the problems associated with cybercrime cases are likely to increase with it. Through the findings of this study, we have underlined the difficulties in dealing with cybercrime cases – issues like inadequate and ambiguous laws, lack of skilled investigators and expert judges, centralized jurisdiction of Kathmandu District Court, and enforcement challenges. Therefore, this research paper was a small step towards understanding the cybercrimes

cases in Nepal so that we may understand the underlying problems existing in the legal regime and consequently, find solutions that bridge the gap so identified, leading to proper and effective implementation and enforcement of cybercrime laws in Nepal.

Bibliography

Books and Articles

1. Bashu Dev Phulara, *Crime: Tackling Cybercrime in Nepal*, The Nepal Digest, 2004.
2. Creole Palmer et al., *Cyber Crime – A New Breed of Criminal,* 2003.
3. Debarati Halder and K. Jaishankar, *Cyber Crimes against Women in India*, 2017
4. Dr. Tarbez Ahmed, *Nature and Scope of cyber law,* 2018.
5. Lon Fuller, The Internal Morality of Law (1964).
6. M Dasgupta, *Cyber Crimes in India: A Comparative Study*, 2009.
7. Narayan Prasad Sharma, Cyberspace and the Cyber Law, 2015.
8. Shri Krishna Bhattarai, *Social Media related Cybercrime in Nepal and its Legal remedy*, 2016.

Table of Statutes

1. The Constitution of Nepal, 2072
2. The Electronic Transaction Act, 2063
3. *Muluki* Penal Code, 2074
4. *Muluki* Criminal Procedure Code, 2074
5. Indian Information Technology Act, 1996
6. Information Technology Bill, 2075

Miscellaneous

1. Annual Report of the Supreme Court, 2076/77
2. By the editorial. “Zoom bombing disrupts Nepal Tourism Board video conference.” The Himalayan Times. (June 2020)

   https://thehimalayantimes.com/kathmandu/zoom-bombing-disrupts-nepal-toursim-board-video-conference
3. By the editorial. “Journalist arrested for an online news story.” My Republica (September 2019)

   https://myrepublica.nagariknetwork.com/news/journalist-arrested-for-online-news-story/
4. Ganguly Shreya. “Nepal Comedian Pranesh Gautam released from jail after 9 days on district court order”. Medinama (June 2019).

   https://www.medianama.com/2019/06/223-nepal-comedian-pranesh-gautam-
5. Aryal Mina. “Nepal to sign International Cybercrime prevention convention soon.” ICT Frame (February 2018).

   https://ictframe.com/nepal-to-sign-international-cybercrime-prevention-convention-soon/

Annexure-1

S.N.	Year	Section	Case Name	Case Number	Conviction/Acquittal	Nature of Cybercrime	Remarks
1	2076	47	GoN (FIR of Bidha Choudhary) v. Kamala Himal and Priya Smriti Dhakal	075-C1-0243	Penalty of 10,000 as well as compensation of 25,000	Online defamation	Posted video on porn site
2	2076	47	GoN (Geeta Oli) v. Laxmi Oli	075-C1-2471	Compensation of 25,000	Online defamation	Posted hateful words on Facebook
3	2076	47	GoN v. Shambhu Sunwal	076-C2-0011	Compensation of 25,000	Blackmail	Sends girl's naked pictures to her father
4	2076	47	GoN (Shrinkhala Khatiwada) v. Dhak Bahadur Karki	076-C2-0091	Compensation of 5,000	Harassment	Messages via different social media platforms
5	2076	47	GoN (Suchita Basnet) v. Sameer Karki	073-C2-0024	Penalty of 15,000 as well as compensation of 50,000	Harassment	Vulgar posts and photos
6	2076	47	GoN (Manisha Joshi) v. Rajendra Prasad Bhatta	075-C1-1774	One year imprisonment; with penalty of 50,000 as well as compensation of 1,00,000	Blackmail and Online defamation	Send obscene videos and pictures to girls family

7	2076	47	GoN (Name undisclosed) v. Kushsehor nath Jha	075-C1-0954	One month imprisonment; with penalty of 20,000 as well as compensation of 25,000	Threats	Threatening messages on Facebook
8	2076	47	GoN (FIR of Kuar Shri Khatri) v. Dr. Megh Raj Tiwari	074-C1-0576	Penalty of 30,000 as well as compensation of 40,000	Harassment	Posted vulgar message on FB
9	2076	47	GoN v. Hari Prasad Manandhar	075-C1-0669	Imprisonment of 40 days with compensation of 25,000	Fake News	Spread false news and pictures of person's death
10	2076	45 + 44	GoN (Himal Tamang) V. Pramod Dahal	075-C1-0038	Imprisonment of 25 days with compensation of 10,000	Destruction of source code	Destroys IMEI number of sim cards
11	2075	47	GoN (Meena Thapa) V. Tek bahadur Biswokarma	074-CR-1592	Acquitted	Blackmail	False prosecution – case filed under duress
12	2075	47	GoN (Bidhya Shahi) V Shyam Kumar Pahari	074-CR-1822	Imprisonment of 30 days	Online defamation	Posted vulgar photos on FB
13	2075	47	GoN (Anand Niraula) V Rakesh Kumar Giri	074-CR-0818	Penalty of 30,000	Harassment	Victim is foreign citizen

14	2075	47 + 58	GoN (FIR of Shambhu Dayal Agrawal) v. Shobha Karki	074-CR-1662	Imprisonment of 20 days with compensation of 25,000	Blackmail and defamation	Records video illegally then demands money
15	2075	47	GoN V. Hari Prasad Manandhar	074-C1-0639	Imprisonment of 40 days with penalty of 25,000	False news	Posts dead pic of Prime Minister
16	2075	47	GoN (Monica Shrestha) V Bikram Malla Thakuri	075-C1-0047	Imprisonment of 30 days with penalty of 30,000	Fake FB Identity and harassment	Repeated offender
17	2075	47	GoN (Puja KC) V Roshan Deuja	074-CR-1505	Imprisonment of 25 days; penalty of 30,000 as well as compensation of 50,000	Online defamation	Sex tape posted in FB
18	2075	47	GoN (Mina Thapa) V Sunita G.C.	074-CR-1828	Imprisonment of 45 days; penalty of 15,000 as well as compensation of 5,000	Online defamation	Photoshopped and posted nude pics
19	2075	47	GoN (Nirajan Bahadur) V Jokh Bahadur Shah (Ujjar)	074-CR-1122	Acquitted	Online defamation	False rumours
20	2075	47	GoN (Dr. Priya Rimal) V. Pravantra Kuymar Goit	074-CR-1593	Compensation of 10,000	Harassment	Constant calls and messages for 4 Years

21	2075	47	GoN (Swikriti Ghimire) V Dhundi Raj Basnet	074-CR-0895	Imprisonment of 20 days; penalty of 10,000 as well as compensation of 5,000	Harassment	Sends vulgar messages
22	2075	47	GoN (Chanda shree) V. Bhishal Gharti	074-CR-1856	Acquitted	Blackmail and harassment	Hostile witness and lack of evidence.
23	2074	47	GoN (Interpol's FIR) V Kumud Prasad Shah	074-CR-094	Imprisonment of 15 days and penalty of 35,000	Threat and harassment	Victim is Australian
24	2074	47	GoN (Mina Kumari Kharel) V Mahesh Kumar Rana Magar and others	074-CR-0737	Penalty of 25,000 as well as compensation of 50,000	Online defamation	Defaming business organization
25	2074	47	GoN V Dev Raj chaulagai and Ranju Shakya	074-CR-0131	Imprisonment of 15 days; penalty of 10,000	Online defamation	Posts vulgar pictures and words using fake account
26	2074	45	GoN (C.I.B) V. Yogandra Bimali	074-CR-0160	Penalty of 10,000	Unauthorized access	Accesses FB messages during phone repair
27	2074	47	GoN (Punam B.K.) V Saroj B.K. Khadka	074-CR-0469	Acquitted	Online defamation	Lack of evidence
28	2074	47	GoN (Pabitra Pun) V Deepak Lal Shrestha	074-CR-0252	Imprisonment of six months; penalty of 20,000 as well as	Online defamation	Posts nude pictures on FB

					compensation of 50,000		
29	2074	47	GoN (FIR of Hari Ram Bhandari) V Pabam Bi.Ka	073-CR-0569	Penalty of 25,000 as well as compensation of 25,000	Defamation and harassment	Victim is from New Zealand
30	2074	47	GoN V Pratap Malla	073-CR-1480	Penalty of 5,000	Online defamation	Posts Defamatory posts about President
31	2073	47	GoN v. Ranjit mishra and pramod upadhyaya	071-CR-1343	Penalty of 25,000 for Mishra, Pending for Upadhyay	Blackmail	Blackmail to upload photos on FB; Pending because accused in US
32	2073	47	GoN V. Pareshwor Kharel	071-CR-1306	Acquitted	Blackmail	Threat to disclose confidential information of company – No publication
33	2073	45	Nepal Army Authorized Department (FIR) v. Undisclosed name	072-CR-0764	Acquitted	Hacking and unauthorized access	Accused is a minor
34	2073	47	GoN (Prasahant Shrestha) V Ram Kumar Shrestha	073-CR-0743	Penalty of 10,000 with also compensation of 50,000	Fake news	Spread false rumours of a death of a person

35	2073	52	GoN (Aditi Shrestha) V Bikash Kumar Shah	073-CR-0378	Acquitted	Fake identity and fraud	Forensic lab disproves defendant's involvement
36	2073	47	GoN (FIR of CBI) v Ram Avatar Yadav	072-CR-3226	Acquitted	Online defamation	Defames Prime Minister – Lack of evidence to prove claim
37	2073	47	GoN (Homnath Dharel) v Suresh Shrestha	072-CR-3538	Acquitted	Defamation	Posted marriage video on porn site – Court only looks at content, not website
38	2073	47	GoN (Sadikshya Adhikari) V Narayan Paudel	073-CR-0395	Acquitted	Online defamation and harassment	Posted only in Private Domain
39	2073	47	GoN (Manila Mali) V Krishna Uraw	072-CR-0084	Imprisonment of 24 days; penalty of 5,000 as well as compensation of 10,000	Harassment	Threats in SMS
40	2073	47	GoN (Nirmal Kumar Shrestha) V Prakash Basukala Dangol	071-CR-1166	Dismissed	Defamation	Convert to defamation
41	2073	47	GoN(FIR of Sabina Thapa) v Subash Kumar	072-CR-3169	Acquiited	Online defamation	Only personal messages

42	2073	44 + 45	GoN (FIR of Police report) v. Bikash Paudel	072-CR-3360	25 days imprisonment with penalty of 30,000	Hacking	Government office website hacked
43	2073	47	GoN v. Khimanand KC	072-CR-2342	30 days imprisonment with compensation of one lakh. Also, codification of any such electronic devices.	Online defamation	PM and President meme
44	2073	44	Raj Mandhar FIR v. Prem Bahadur	072-CR-3517	23 days imprisonment with compensation of one lakh. Also, codification of any such electronic devices.	Hacking	Hacked Image Channel website and merges it with Viral Khabar.
45	2072	44 + 45	GoN (FIR of Ministry of Health and Population's letter) v Prakash Bhatta	071-CR-0075	Acquitted	Unauthorized Access	Intention to check internal security, not to steal any confidential information
46	2072	47	GoN (FIR of Deepa Khadka) v Shyam Bahadur Sarki	071-CR-1348	Penalty of 5,000	Online defamation	Uploads vulgar photos on FB
47	2072	45	GoN (FIR of bhupesh Karki) v Awesh Gautam	070-CR-2228	Penalty of 5,000	Unauthorised access	Using company email even after leaving job

48	2072	47	GoN (FIR of Savitri Khadka) v Devendra Khatri	072-CR-214	Six months imprisonment; penalty of 25,000 as well as compensation of 50,000	Blackmail and harassment	Threatening and vulgar SMS texts
49	2072	47	GoN (FIR of Pushkar Chaudhary) v Deepak Kumar Das	070-CR-1963	Acquitted	Fake ID and Defamation	Lack of evidence, the accused has an alibi.
50	2072	52	GoN (FIR of Sushil Kumar Rao) v Prabin Karmacharya	070-CR-1810	Penalty of 25,000 plus recovery of stolen amount	Online theft and fraud	Diverts and steals money online from Kantipur Media.
51	2072	45	GoN (FIR of Police report) v Raju Shrestha	071-CR-2039	Acquitted	Fraud	Fraud not covered by section 45 – wrong prosecution
52	2072	45 + 47	GoN (FIR of Police report) v Bishal G.C and ors	071-CR-1944	Penalty of 2,000	Blackmail and hacking	Hacked into victim's account and blackmailed
53	2072	47	GoN (FIR of Police report) v Nikhil Maharjan	071-CR-1840	Penalty of 5,000 as well as compensation of 25,000	Harassment	Vulgar messages and photos on Viber
54	2072	47	GoN (FIR of Police report) v Rahul Balmiki	072-CR-0086	Acquitted	Blackmail	Only private conversation

55	2072	47	GoN (FIR of Lalit Kumar Agrawal) v Biswanath Acharya	071-CR-2071	5 months imprisonment	Blackmail and Threat	Sends threatening emails to the news network
56	2071	47	GON V Mukunda Ghimire	070-CR-1996	Acquitted	Harms national integrity	Accused changes the shape of national flag and posts online
57	2071	47	GON (Ganga Kumari Pun) V Ambraj Dalla koti	072-Cs-0802	Pending	Fake email and Online defamation	Accused not yet caught
58	2071	47	GON (SC's FIR) V Prabhat Kumar Gupta	072-Cs-0802	Acquitted	Unauthorized filming and recording	Illegal recording of conversation – not covered by Section 47.
59	2071	47	GoN (Kumari Khanal) V. Kapil Dev Thapa	070-CR-0766/182	Acquitted	Threats	Statutory Limitation crossed
60	2071	47	GoN (Eliza Shrestha) V. Saroj Bhuju	070-CR-2053	Acquitted	Harassment and Defamation	Lack of evidence, only suspicion
61	2071	45 + 47	GoN ((Ranju Sharma) V. Biswas Shrestha	22-39-069-2667	Acquitted	Hacking and Defamation	Private domain – Husband to wife
62	2071	47	GON(Krishna Mor) V Ram Kumar Shyangba	071-CR-0421	Acquitted	Fake Id and Harassment	Inconclusive proof
63	2071	45 + 47	GoN (Sambhranata Karki) V Surendra Raut	070-CR-1623	Imprisonment of one year; penalty of 20,000 as well as	Fake Id and Catfishing	Posing as a girl and posting vulgar photos

					compensation of 40,000		
64	2071	47	GoN (Smjhana Mahat) v. Evan Joshi	070-CR-2000	Penalty of 30,000 as well as compensation of 10,000	Harassment	Posts vulgar messages
65	2070	47	Gon (Kalpana Bista) v. Kabin Karki	070-CR-0340	Penalty of 10,000	Online defamation	Published vulgar pictures and phone number through fake account
66	2070	47	Gon V. Bhawanath Sapkota	3108/2069 (22-39-069-31087)	Acquitted	Defamation	Did not post anything, only liked a status.
67	2070	45	GoN (FIR from Broadlink admin head) V Subash Chandra Paudel and ors.	2675/2075	Acquitted	Unauthorized access and theft	Information was available openly – no intention to steal
68	2070	47	GoN V. Ravi Kumar Kesari	1391 /2069	Penalty of 30,000	Online defamation	Video published from cybercafe – owner arrested
69	2069	47	GoN (Hima Bhattrai) V Megh Raj Timalsina	2642/430	Imprisonment for six months with penalty of 25,000	Harassment and Defamation	Posted vulgar message and photoshopped images

70	2069	52	GoN V Kirtan Pokharel	1372/2069	Imprisonment for 2 months with penalty of 25,000	Fake website and fraud	Targeting minors in New Zealand.
71	2069	45 +46	GoN V Nigele Johnpogomere and Jiggy Gaton	39-067-1472	Pending	Data Theft, phising and fake website	Stealing data by creating fake website
72	2069	47	GoN V Raj Rai	2771/2069	Acquitted	Online defamation	Drugged the victim and took nude pictures – later posted online
73	2069	47	GoN (Berger and Nerolac) V Suresh Sharma Adhikari	2550/2069	Acquitted	Data Leak	Leaked confidential information of company after dismissal
74	2068	47	GoN V Tej Raj Joshi	2750/2068	Penalty of 10,000	Harassment	Repeatedly changed numbers and harassed girl
75	2068	47	GoN (Reema Subedi) V Pradeep K.C.	1341/2068	Penalty of 21,000	Defamation	Send nudes from email
76	2068	47	GoN V Dilli Nath Subedi	1556/2068	Penalty of 2,000 as well as compensation of 15,000	Online defamation	Drugged and clicked naked pictures then posted online
77	2068	47	GoN (Aarya Gautam) V Saroj K.C	1809/2069	Penalty of 20,000 as well as compensation of 25,0000	Defamation	Unknowingly taking pictures and posting online

78	2068	47	GoN V Prabin Prajapati	2188/2069	Imprisonment of six months; penalty of 10,000 as well as compensation of 10,000	Online defamation	Posted sex tape online
79	2067	47	GoN (Ham Bahadur Gurung) V Hari Panta	070-CR-0146	Acquitted	Defamation	Convert to defamation
80	2067	47	GoN (Shova K.C) V Bhoj Raj Lingden	39-067-1430	Acquitted	Blackmail and Defamation	Inconclusive proof – lack of evidence