WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Legal Frameworks and Penalties for Cyber Extortion: A Comparative Analysis of India And Global Perspectives

***Charu Chadha[1], Dr. Prashant Kumar Varun[2]***

[1]ICFAI Law School, The ICFAI University, Dehradun charuchadha9@gmail.com
[2]Assistant Professor, ICFAI Law School, The ICFAI University, Dehradun prashant.kumar@iudehradun.edu.in

**ABSTRACT**

Cryptoviruses, where the data is held hostage under threat of leak, emerge as the main risk factor in contemporary world where everyone is connected. The current article introduces legal provisions governing cyber extortion in India as well as other countries and underscores the prominence of understanding and thorough implementation of the edict to curb the crime. The research which is being employed in this study is largely doctrinal, using secondary sources to investigate the laws and punishments about cyber blackmail apart. The research circle, as in the case of India and other countries, will be made visible by means of the consideration of the potential penalties in this case, either light, moderate or severe. Thus, this study is not only significant but it also assists in raising the level of cyber extortion crimes which has developed together with technology being always on the increase. This dissertation tackles the origin of cybercrime and its many forms including financial fraud, intellectual property theft, and cyberstalking. The discussion at the end of this dissertation shows the complex nature of this danger. The Digital India Program that is India-specific has impediments such as cybercrime frauds which has become a part of the society. Statistics from the National Crime Records Bureau are attached with a trend of a growing number of cyber-crime cases which though requires some strong legislation to deal with such offences effectively. In that sense international collaboration is of a vital importance in the fight against cybercrime because criminalistic groups are always taking evolvement into account and are assisted by differences in legal frameworks of different states. There are different types of international responses, as various institutions highlight offenses in their conventions and model laws, which have the aim of making the international community's efforts to combat cyber blackmail consistent. The enactment of the Information Technology Act of 2000 in India has been a crucial pivot point for cyber security awareness and dealing with cybercrime, with challenges like uniform positive laws for the internet and adequate enforcement aspects still knotting the issue. Recommendations could include extradition treaties and classic legal systems updating in order to absorb cyber challenges and their new nature.

**Key Words: cyber extortion, Legal framework, cybercrimes, cyber security, Unified internet laws, Criminal Penalties**

## 1. Introduction

Cyberextortion is a criminal activity that entails an attack or threat of attack combined with a demand for money to avert or terminate the assault. This type of malware, known as ransomware, encrypts user documents on infected computers with its destructive code and then demands a payment for the key needed to unlock them. While many people's understanding of "cyber extortion" is poor. Given the increasing amount of information interchange in our society through internet, this kind of crime has the potential to have a significant negative influence on both our personal lives and society as a whole. As such, it is imperative that the subject of "cyber extortion" be thoroughly introduced, with a particular emphasis on the legal frameworks governing India and other nations.

### *A. Research Methodology*

The facts and interpretations used in this study are foundational. The research and writing are grounded in secondary facts derived from the current laws that have been enacted both domestically in India and internationally. As such, the inquiry is doctrinal in character.

### *B. Scope of Research*

The laws that are in place in India and other nations, as well as the punishments for these crimes, will be the primary topics of this dissertation.

### *C. Significance*

This study is significant because, ever since there have been crimes, individuals have exploited extortion as a way to obtain money. But prior scams typically included harm to pricey objects or sometimes the victims themselves. Despite this, con artists of this kind are still highly prevalent in the modern world. Consequently, raise your awareness of this crime. This is a crucial piece of study.

### *D. Research Questions*

1. Are the penalties for cyber extortion strict in India?
2. What are the differences in the laws of India and other countries for this crime?

## 2. Origin of Cyber Crime

The first cybercrime occurred in 1820! Since the abacus, the earliest computer, was invented in India, Japan, and China about 3500 BC, this is not unexpected. Modern computers originated with Charles Babbage's analytical engine.

The loom was invented by French textile maker Joseph-Marie Jacquard in 1820. This equipment repeated weaving procedures for unique materials. Jacquard workers worried about their jobs and livelihoods. They sabotaged Jacquard to stop him from using the new technology. This is the first recorded cybercrime.

Neural networks and nanocomputing might convert every particle in a glass of water into a billion-operation-per-second computer.

Modern life's growing computer dependency has led to cybercrime. In an age where everything from microwave ovens and refrigerators to nuclear power plants are driven by computers, cybercrime has taken on extremely grave overtones. Recent cybercrimes include the Citibank fraud. $10 million was illegally moved from the bank to a bank account in Switzerland. A Russian cyber squad commanded by Vladimir Kevin, a known hacker, carried out the attack. The gang penetrated the bank's security systems. Vladimir was reportedly using his workplace computer at AO Saturn, a computer business in St. Petersburg, Russia, to sneak into Citibank's systems. He was finally apprehended at Heathrow airport as he proceeded to Switzerland.

Types of cyber crimes

A basic but powerful definition of cybercrime would be "illegal acts in which the computer is a tool, a target, or both."

Let's examine the acts in which the computer is a tool for an illegal act. This type of activity usually involves a modification of a conventional crime through the use of computers. Some examples are:

*A. Financial Crimes*

This might involve cheating, credit card fraud, money laundering, etc. To quote a recent scenario, a website claimed to sell Alphonso mangoes for a throwaway price. Wary of such a transaction, relatively few customers answered or gave the website with their credit card data. In actuality, these folks were sent Alphonso mangoes. News about this website has spread like wildfire. Thousands of people around the country reacted and ordered mangoes by submitting their credit card details. The operators of what was ultimately discovered to be a phoney website fled taking the countless credit card information and continued to spend significant sums of money much to the disgust of the card owners.

*B. Sale of Illegal Articles*

This might mean sending emails, posting content on message boards, auction websites, and websites selling narcotics, weapons, and animals, among other things..

*C. Online Gambling*

Millions of websites provide online gambling, and all of them are hosted on servers located abroad. Many of these websites are really believed to be fronts for money laundering.

*D. Intellectual Property Crimes*

Millions of websites provide online gambling, and all of them are hosted on servers located abroad. Many of these websites are really believed to be fronts for money laundering..

*E. Email Spoofing*

A fake email is one that seems to be from one source but was really received from another. Beza's email address, for instance, is beza@bezaspeaks.com. His enemy Dorexi uses a forged email address to deliver explicit messages to everyone she knows. Since Beza seems to be the source of the emails, his friends and business partners may take offence and their ties may suffer irreversibly.

Email spoofing may potentially cause financial harm. One case included a teenage American who made millions of dollars by spreading rumours about companies whose shares he had shorted. This fraudulent information was spread by emailing investors and stock brokers with phoney letters that seemed to be from news agencies like Reuters, informing them that the companies were collapsing. Even when the truth was revealed, thousands of investors suffered significant financial losses since the share prices did not rise back to their prior levels.

*F. Forgery*

With the use of advanced computers, printers, and scanners, counterfeit money notes, revenue stamps, postage, mark sheets, and other materials may be produced. Computers, along with top-notch printers and scanners, are used in their production. In reality, this has grown into a lucrative industry, with student gangs receiving thousands of Pula in return for these phony-looking but real credentials.

*G. Cyber Defamation*

This happens when someone defames someone using a computer and/or the Internet. For instance, someone may post disparaging material about someone on the internet or send disparaging emails to all of that person's acquaintances..

*H. Cyber Stalking*

"Stalking" is defined as "pursuing stealthily" by the Oxford Dictionary. Cyberstalking is tracking a person's online activities by sending unsolicited and occasionally threatening posts on the message boards the victim frequents, joining the chat rooms the victim frequents, sending unsolicited emails to the victim, and so on.

## 1. Indian Scenario

To the best of its ability, India is attempting to carry out the Digital India bad track record initiative. The Digital India initiative will only be successful if there is maximum connection and no chance of cyberattack. Given its lack of cyber security, India is also affected by this.

Home Ministry figures show that 22,060 cyber fraud crimes were registered in 2012, compared to as high as 71,780 instances reported in 2013. Up to June 2014, there have been 62,189 instances of cyberfraud.

In 2013, many hacker organizations located all over the world compromised 28,481 Indian websites. In 2012, there were 27,605 hacking incidents, up to 21,699 in 2011.

According to the National Cyber Records Bureau's cybercrime data, the Information Technology Act was used to record 1,791, 2,876 and 4,356 incidents in 2011, 2012 and 2013, respectively. In 2011, 2012, and 2013, the Indian Penal Code's provisions pertaining to cybercrime resulted in 422, 601 and 1,337 cases being lodged, respectively.

The National Crime Records Bureau (NCRB) reports that during the last two to three years, there has been an annual increase in cybercrime cases registered in the nation of more than 40%. A total of 288, 420, 966, 1,791 and 2,876 cybercrime cases were registered under the IT Act during 2008, 2009, 2010, 2011, and 2012, respectively. Based on data compiled and monitored by the Indian Computer Response Team (CERT-In), 308, 371, and 78 government websites were compromised in 2011, 2012, and 2013, respectively. In 2013, 16,035 incidents pertaining to spam, malware infection, and system intrusion were reported.

## 2. Global Scenario

The efficacy of both national and international legislation and law enforcement is frequently called into question by international cybercrimes. Due to the fact that many nations' current legal frameworks are not designed to address cybercrime, criminals are increasingly turning to the Internet to commit crimes in order to avoid facing harsher penalties or having it more difficult to track them down. Governments and businesses, whether in wealthy or developing nations, have progressively come to understand the enormous risks that cybercrime poses to public interests, political and economic security, and both. Retaliation becomes more challenging, though, as cybercrime becomes more sophisticated in its manifestations. In this way, worldwide collaboration is necessary to combat cybercrime. Already, a number of nations and organizations have worked together to create international law enforcement and legislative norms at both the regional and global levels. Since China and the United States are the two main nations from which cybercrime originates, their collaboration is one of the most notable recent developments.

ICT, or information and communication technology, is crucial in promoting security and interoperability based on international standards. In order to combat cybercrime, general countermeasures have been implemented. These include technical and legal measures to improve legislation, Internet content control, the use of public or private proxies, computer forensics, encryption, and plausible deniability. This article will mostly focus on legislative and regulatory attempts of international cooperation due to the diversity of law enforcement practices and technological countermeasures between nations.

*I. International Trends*

Criminals are shifting from simple adventure and vandalism to more focused attacks as they become more aware of the potentially significant financial gains that can be made through cybercrime. This is especially true of platforms like computers, mobile devices, and the Cloud where valuable information is concentrated. Cybercrime is on the rise globally, with many tendencies emerging.

- *Platform switch:* Mobile phones, tablet computers, and VoIP are becoming new platforms for cybercrime to fight on, replacing Windows-based PCs. because there is now a noticeable threshold for vulnerabilities. By offering quicker updates, patches, and user alerts for any vulnerabilities, PC manufacturers are improving the security of their systems. Furthermore, by 2013, there will be more than 1 billion mobile devices worldwide—from smartphones to tablet PCs—accessing the Internet, which will increase the potential for cybercrime. Zeus, the wildly popular banking Trojan, is already being optimized for mobile devices. Another technique used by cybercriminals to take advantage of mobile devices that people download after falling for a social engineering scam is known as "smishing," or SMS phishing. Its goal is to circumvent the SMS-based two-factor verification that most banks employ to validate customers' online money transactions. The use of VoIP technologies to facilitate the increasingly common practice of vishing (telephone-based phishing) schemes.

- *Social engineering scams:* It is a non-technical type of infiltration that mostly depends on human interaction, such as emails or social networking chats, and frequently includes tricking prospective victims into installing malware or disclosing personal information. Nonetheless, social engineering is a very powerful tool for using trust to breach secure computer networks. Cybercriminals are using social networking sites more and more to find money mules to help with their money laundering schemes all around the world. In addition to using fake social media posts to trick recipients into clicking on links in emails, spammers often use people's confidence in their social media relationships to draw in new victims.
- *Highly targeted:* Malware designed to interfere with industrial systems, like the Stuxnet network worm that takes use of Microsoft's zero-day vulnerabilities, is the most recent development in the "hypertargeting" space. In a German plant, the worm's first known duplicate was found. A later variation caused a worldwide outbreak that spread widely.

*Dissemination and use of malware:* Malware often manifests as spyware, worms, Trojan horses, or viruses. Malware links to host websites registered in the United States of America (51.4%) more often than in China (17.2%) or Spain (15.7%) in 2009. Email is one of the main channels via which malware is spread. Its reach is genuinely global.

- *Intellectual property theft (IP theft):* An estimated $600 billion is traded in counterfeit goods globally annually, with 90% of software, DVDs, and CDs marketed in some countries being fake. IP theft is expected to cost businesses $250 billion a year and 750,000 jobs in the USA alone..

### *J. International Responses*

*G8:* The leaders of the eight industrialized nations that make up the Group of Eight (G8) are the United States, the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

A Ministers' Communiqué was issued by the G8 in 1997, containing principles and an action plan for fighting cybercrime and safeguarding systems and data from unauthorized modification. In addition, the G8 requires all law enforcement officials to be prepared to handle cybercrime and appoints a point of contact for each of its member nations that is available around-the-clock, seven days a week.

- *United Nations:* The UN General Assembly passed a resolution in 1990 that addressed laws pertaining to computer crime. A resolution against the illegal abuse of information technology was approved by the UN GA in 2000. A second resolution on the unlawful exploitation of information technology was approved by the UN GA in 2002.
- *ITU:* Leading the way in the development and standardization of telecommunications and cybersecurity challenges is the International Telecommunication Union (ITU), a specialized institution under the United Nations. The World Summit on the Information Society (WSIS) was headed by the ITU.

The Geneva Plan of Action and the Geneva Declaration of Principles, which were published in 2003, emphasize the need of taking action in the battle against cybercrime. The Tunis Agenda and the Tunis Commitment were approved in 2005 for the Information Society.

- *Council of Europe:* The Council of Europe is a global organization that aims to promote democracy and human rights among its 47 member nations in Europe. The first international treaty targeting cybercrime was the treaty on Cybercrime, which was signed by 46 member nations in 2001. The Convention was co-drafted by the Council of Europe, the United nations, Canada, and Japan. However, only 25 nations ratified in the end. Through standardization of cybercriminal offenses qualifying, provision for legislation empowering law enforcement, and facilitation of international collaboration, it intends to provide the foundation for an efficient legal framework for combating cybercrime.

## 3. Cyber Law in India Global Scenario Penalties in India and in Different Countries

### *A. Emergence of Information Technology Act, 2000*

The United Nations General Assembly Resolution A/RES/51/162, dated January 30, 1997, which endorsed the Model Law on Electronic Commerce by the United Nations Commission on International Trade Law, led to the enactment of the Information Technology Act 2000 in India. This was the first step toward the creation of an international e-commerce law that would govern an alternate mode of trade and grant the sector legal status. It was passed while keeping in mind the 1996 UNICITRAL model of e-commerce law.

- A Few Notable Sections of the Information Technology Act of 2000.
- Section 43: Compensation for Rupees One Crore for Computer System Damage, etc.
- Hacking (with purpose or knowledge) under Section 66: a fine of two lakh rupees and a three-year jail sentence.
- Section 67: Publication of pornographic content in electronic form carries a fine of one lakh rupees, a five-year jail sentence, and a double conviction for a second offense.
- Sec. 68: Failure to follow controller instructions may result in a fine of up to Rs. 2 lakh and a 3-year jail sentence.
- Sec. 70: Penalties for trying or obtaining computer access include up to ten years in jail.
- Sec. 72: Penalties for violating computer information confidentiality include a fine of up to Rs. 1 lakh and up to two years in jail.

- Section 73: misleading digital signatures and misleading information published online may result in a fine of one lakh rupees, two years in jail, or both.
- Section 74: Publication of Digital Signatures for Fraudulent Purposes - A punishment of one lakh rupees and two years in jail.

*B. International Cybercrime Conventions*

- Convention on Cyberspace Security and Protection of Personal Data of the African Union;
- Convention on Cybercrime of the Council of Europe (commonly known as the Budapest Convention on Cybercrime).

*Model Laws:*

- CW Model Law – Model Law on Computer and Computer- related Crime
- SADC Model Law – SADC Model Law on Computer Crime and Cybercrime
- HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbeans (Cybercrime/e- Crimes)
- ITU – International Telecommunications Union Cybercrime Legislation Resources – ITU Toolkit for Cybercrime Legislation

*Some specific cybercrime law:*

- Cybercrimes and Cybersecurity Bill (Cyber Bill) – South Africa (South Africa signed the Budapest Convention in 2001)
- Cyber security Information Sharing Act (CISA) – United States of America (this Bill has recently been passed by the US Senate)
- EU Network and Information Security Directive
- Criminal Code Act 1995 Australia
- Cybercrime Act 2001 Australia
- Chapter 08:06 (Cybercrime and Computer- related Crimes) Botswana
- Computer Misuse Act, 2007 Brunei Darussalam
- Criminal Code of Canada, Canada
- Cyber security Law China
- Criminal Code France
- Computer Crimes Act Malaysia
- Crimes Act,1961 New Zealand
- Cybercrime Prevention Act of 2012 – Philippines
- Act on Computer Crimes Thailand
- Cybercrimes Act, 2015 Tanzania
- UK – Computer Misuse Act, 2013
- United States Code USA

## 4. Conclusion

There is no denying the usefulness of the internet in today's society, be it in the political, economic, or social spheres. Though there are advantages and disadvantages to everything, cyberterrorists have seized control of technology for their own gain. The Information Technology Act of 2000, which is based on the UNICITRAL model of e-commerce law, was created to curtail their operations. It has numerous benefits, such as providing legal recognition to electronic records and transactions, certifying and authenticating digital signatures, preventing computer crimes, and so on, but it also has a number of disadvantages, such as not protecting intellectual property rights, domain names, cyber-squatting, and other issues. Corporate entities are discouraged from investing in the infrastructure of information technology as a result. Incidents such as Dawood and Quattrochi make the issue with India's enforceability mechanism very evident. A recent development in the security of sensitive data is cryptography. Nowadays, there aren't many businesses using this technology. Cybercrimes continue to represent a threat to millions of others.

To minimize ambiguity in their implementation, internet laws urgently need to be unified. For example, we have the Indian Penal Code (IPC), the Obscenity Law, the Communication Decency Law, self-regulation, the Information Technology Act 2000, the Data Protection Act, the Criminal Procedure Code, and so on, but they lack an effective enforceability mechanism because they address the issue in an ambiguous manner. There is uncertainty over the application of the several laws addressing the topic because none of them clearly address it in its entirety. I would propose unifying

laws by taking all internet laws to create a code that is effective enough to deal with all of the following: • Cybersecurity Information Sharing Act (CISA) - United States of America (this Bill has recently been passed by the US Senate) in order to end the confusion in applicability of Legislation picking from various laws to tackle the problem.

• Directive on Network and Information Security of the EU

• Australia's Criminal Code Act of 1995

• Chapter 08:06 (Cybercrime and Computer-related Crimes) of the Cybercrime Act 2001 of Australia Namibia

• Brunei Darussalam's 2007 Computer Misuse Act

• The Criminal Code of Canada

• China's Cybersecurity Law

• France's Criminal Code

The Malaysian Computer Crimes Act and the 1961 Crimes Act in New Zealand

• The Philippines' Cybercrime Prevention Act of 2012

Act on Computer Crimes, Thailand; Tanzania's Cybercrimes Act, 2015

UK's Computer Misuse Act of 2013 and the USA's United States Code

## 6. Final Thoughts

There is no denying the usefulness of the internet in today's society, be it in the political, economic, or social spheres. Though there are advantages and disadvantages to everything, cyberterrorists have seized control of technology for their own gain. The Information Technology Act of 2000, which is based on the UNICITRAL model of e-commerce law, was created to curtail their operations. It has numerous benefits, such as providing legal recognition to electronic records and transactions, certifying and authenticating digital signatures, preventing computer crimes, and so on, but it also has a number of disadvantages, such as not protecting intellectual property rights, domain names, cyber-squatting, and other issues. Corporate entities are discouraged from investing in the infrastructure of information technology as a result. Incidents such as Dawood and Quattrochi make the issue with India's enforceability mechanism very evident. A recent development in the security of sensitive data is cryptography. Nowadays, there aren't many businesses using this technology. Cybercrimes continue to represent a threat to millions of others.

To minimize ambiguity in their implementation, internet laws urgently need to be unified. For example, we have the Indian Penal Code (IPC), the Obscenity Law, the Communication Decency Law, self-regulation, the Information Technology Act 2000, the Data Protection Act, the Criminal Procedure Code, and so on, but they lack an effective enforceability mechanism because they address the issue in an ambiguous manner. There is uncertainty over the application of the several laws addressing the topic because none of them clearly address it in its entirety. The Information Technology Act is applicable to all individuals, regardless of their nationality (i.e., non-citizens as well), who commit offences under the Act outside of India, provided that the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Sections 1 and 75 of the Act. However, this provision lacks practical value until and unless the person can be extradited to India. In order to end the confusion regarding the applicability of laws, I would suggest unifying all internet laws to create a code that is effective enough to deal with all cases. Thus, it is recommended that nations establish extradition accords. in order to make such clauses practical.

Similar to a "eye for an eye" scenario, the only way to control technology in this case is to comprehend how cyberterrorists have seized control of it. There is no assurance that technology will remain out of the hands of cyberterrorists, even if advancements in it are sufficient to reduce computer-related crime. As a result, countries must modernize their legal systems, either by adopting new ones or by making adjustments. Even though the judiciary is still learning about the nature of crimes using computers, more effective law enforcement mechanisms are desperately needed to keep the system functional.

**References:**


1. https://www.proofpoint.com/us/threat-reference/cyber-extortion#:~:text=Cyber%20extortion%20is%20a%20nefarious,currency%20and%20critical%20infrastructure%20systems. [Visited on 24.04.2024]
2. https://www.indiancybersquad.org/cyber-crime-types [Visited on 22.04.2024]
3. https://www.thehindu.com/sci-tech/technology/digital-financial-frauds-in-india-a-call-for-improved-investigation-strategies/article67988607.ece#:~:text=Cybercrime%20poses%20a%20burgeoning%20threat,crore%2C%20with%204%2C850%20reported%20cases [Visited on 23.04.2024]
4. https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/ [Visited on 22.04.2024]
5. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Visited on 25.05.2024]

6. https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams#:~:text=Social%20engineering%20fraud%20is%20a,by%20telephone%20or%20in%20person [Visited on 24.02.2024]

7. https://blog.ipleaders.in/cyber-crime-laws-in-india/ [Visited on 25.04.2024]