**Sri Lankan and Indian**

**Legal Framework of Cyber-Crime**



**Co-authored by,**

Ruwansarani Ganganathara Uthpala Ranasinghe

ganganathararuwansarani@gmail.com uthpalaranasinghe123@gmail.com

1st year undergraduate 1st year undergraduate

Faculty of Law Faculty of Law

University of Colombo, Sri Lanka University of Colombo, Sri Lanka

 

**Abstract**

**"I am afraid that one-day technology will surpass our human interactions, and then the world will be left with only a generation of idiots."***-Albert Einstein-*

Humans have addicted to use internet unlimitedly with the new technology. High speed internet, technology and smart devices are the positive aspects of the world today. But its negative application is problematic. Because of that many persons have to face cyber bulling. Those things lead to stress, confusion and suicide. Even defining cyber-crime can be tricky. Some researchers say that it is illegal activity which happens in the virtual world. As a broader definition, **any crime facilitated or committed using a computer, network or hardware device is a cyber-crime.** The most prevalent cyber-crimes are abuse, bullying, hacking, identity theft and revenge porn, to more general online criminality, child pornography, e-banking fraud, malware, and phishing etc. Cyber-crimes have been increasing since 2010. It is a global matter and all the countries have activated many rules and regulations for it. Though people are more prone to cyber-crime due to their lack of understanding of the existing laws regarding cyber-crimes. These cyber-crimes have also become a threat to communicate and valuable technological advances that are essential to globalization. The loss of precious lives by a priceless device is a huge social lament.

According to official Sri Lankan police records, traditional street crimes are decreasing but cyber-crimes have been steadily rising over recent years. During the year 2016-2018 India has been ranked as the 2nd amongst the countries affected by cyber-attacks. As closely related countries, we have to pay more and more attention on the legal framework of cyber-crime in India and Sri Lanka.

**INTRODUCTION**

“The computer is rapidly increasing society’s dependence upon it, with the result that society becomes progressively more vulnerable to computer malfunction, whether accidentally or deliberately induced, and to computer manipulation and white colour law-break” It is a well-known saying that “sticks and stones can break your bones but never harm your name.”[[1]](#footnote-1) Although the physical harm of cybercrime is minimal compared to traditional harassment, it can have very detrimental long-term effects on individuals. Emily Moore, a victim of harassment in Britain, said “the Internet was a vicious silent enemy. A faceless computer is more of a threat than a physical bully.” Preliminary research in countries such as China, Canada, The United States, Japan, India, Denmark, Australia, and New Zealand confirms that cyber bullying is a global phenomenon. Cyber bullies often work in groups. Cyber bullies are often former victims of cyber bullying. These are people who are completely confused and like to mess up the lives of others. Cybercriminals post personal data of their victims on websites or publish different information in the name of the victim by pretending to be someone else. Cyber bullies often send threatening messages to their victims on social media, embarrassing them, releasing highly personal information, photos, videos, memes, etc. in public. Cyber bullying victims are mentally disturbed and victims of this harassment are also mentally disturbed. Both the victim and the perpetrator commit suicide because they do not know where to turn for help. Cybercrime has become a social disease. Social awareness of cyber bullying has waned in the belief that cybercrime is just another form of harassment and that nothing on the Internet is real. But it is important to understand that the Internet is full of lies and dark clouds that can confuse anyone, and that social awareness of how to protect oneself from the dangers posed by the Internet is very important.

**Budapest Convention on Cyber-crime**

The convention on cybercrime (also known as the Budapest Convention)[[2]](#footnote-2) is the first international convention out to pursue a common criminal policy against cybercrimes. It promotes the harmonization of national laws, capacity building, and the fostering of International Corporation. The convention was drafted by the Council of Europe and was opened for signatures on 23 November 2001. It entered into force on 1 July 2004.

**The legal framework of Sri Lanka**

**The practicality of cyber-crimes**

Several websites in Sri Lanka have fallen victim to a series of cyber-attacks. According to the **Sri Lanka Computer Emergency Readiness Team** (SLCERT),[[3]](#footnote-3) a group of unknown intruders allegedly attacked numerous Sri Lankan websites, including other websites like Kuwait Embassy in Colombo, the Tea Research Institute in Talawakelle, the Rajarata University in Mihintale, and 10 other private institutions’ websites.[[4]](#footnote-4) SLCERT stated that they’re investigating on the incident combined with the TechCERT and the **Cyber Operations Center** that operates under the Ministry of Defence. CERT told that the number of cybercrimes in Sri Lanka has increased to 8255 within the period of 2019 December to 2020 July, which was a large surge from last year’s cybercrime count of 3562. Among them, 97.4% were social media cybercrimes such as impersonating other people through fake profiles, 0.07% were financial/ email frauds, 0.025% were abuse, hate and privacy violation through phone hacking, and 2.5% were caused by ransomware and phishing. The most cybercrime increase has been seen through social media privacy violation and impersonation through fake profiles as the percentage of social media cybercrime has increased from 74.7% to 97.4% in 2020.[[5]](#footnote-5)

 In Sri Lanka, there have been number of cyber-crime reported to the Sri Lankan Computer Emergency Readiness Team and Cyber-Crime Unit in Sri Lankan police. According to Sri Lankan police records, police mention normal crime rate decreased. But the study analyzes that cyber-crimes gradually increased. Phishing, abuse privacy, malware, e-mail harassment, fake accounts (Facebook, Instagram etc.), and intellectual property cases reported to the Sri Lankan Computer Emergency Readiness Team. In addition to this e-banking cases, website hacking, e-mail harassment, child pornography cases reported to Cyber-Crime Unit in Sri Lanka police. Most of the cases were about fake accounts in Facebook. But under Sri Lankan law, defamation is not considered as criminal offence and it tantamount to a civil matter.

**Legal Conditions**

Computer crimes are considered as a novel aspect in the criminal activities of Sri Lanka. **The Evidence (Special Provisions) Act**,[[6]](#footnote-6) **The Information and Communication Technology Act**,[[7]](#footnote-7) **The Payment and Settlement Systems Act**,[[8]](#footnote-8) **The Electronic Transactions Act**,[[9]](#footnote-9) **The Payment Devices Frauds Act[[10]](#footnote-10)** and **The Computer Crime Act[[11]](#footnote-11)** are the main pieces of legislations which governs the legal regime in the area of Information Technology in Sri Lanka. Computer Crimes Act No. 24 of 2007 primarily addresses computer-related crimes and hacking offences. In this Act, computer crime is a term used to identify all crimes frauds that are connected with or related to computer and Information and Communication Technology Act No.27 of 2003. Recognizing the nature of computer crimes which are committed disregarding boundaries under the Section 2 of the Computer Crime Act courts have a wide jurisdiction to attend the matters irrespective of whether the person resides, the crime was committed or the damage was caused a person or corporation within or outside Sri Lanka. In 2015, as the first country from South Asian region Sri Lanka acceded to the **Budapest Convention**. In line with Article 22 of the Budapest convention, Computer Crime Act covers wide range of application without considering the geographical boarders and nationality. Section **27** enables the extradition of cyber criminals among the states. In Section 3 to Section 10, the Act describes the key substantive offences under Computer Crime Act such as Hacking (illegal access), Cracking, unlawful modification, offences against national security, dealing with unlawfully obtained data, illegal interception of data, using illegal devices and unauthorized disclosure of information which are adequately consistence with the Budapest Convention under the heading of computer integrity offences. Computer Crime Act introduced new procedures in addition to the ordinary criminal procedures and every offence under this Act are cognizable offences Further a significant arrangement is that, government can appoint a panel of experts to assist police officers. Though the Computer Crime Act was enacted before the said accession, the majority of the provisions were in compliance with the Budapest Convention. Some provisions of the Convention were not covered by the Computer Crimes Act such as Child Pornography. The Sri Lankan Penal code has provisions to address this, however, it may not adequate enough to prosecute these crimes when it is committed using Internet. A major challenge in the existing legal framework is that the Computer Crimes Act has failed to identify some of the most common cyber-crime offences, such as illegal gambling, cyber-squatting, hate speech and statements promoting racism, cyber defamation, identity theft, cyber bullying and cyber stalking making it difficult take precautions against such offences.

 The COVID-19 outbreak with the resultant lockdown and stay-at-home measures has led to a surge in online activity by young people. This increased online presence has heightened their susceptibility to online sexual abuse, cyber bullying, exploitation, and other risks.[[12]](#footnote-12)
To address this growing concern and to help combat online hate faced by many youth in Sri Lanka, the ‘Cyber Care’ mobile application was launched recently on **World Safer Internet Day**, commemorated each year on 9 February 2021. The app, which was created by Team Cyberwarders, a team who has successfully completed the incubation phase of the HackaDev: National Youth Social Innovation Challenge aims to help alleviate and prevent cyber violence affecting youth of all genders in Sri Lanka

In Sri Lanka, there have been four main Acts which used in cyber-crime prevention. **1997 computer crime Act** was really important. This Act covers a broad range of offences and it can be divided into two categories. They were computer-related crimes and hacking offences. In Section 3 to Section 10, the authors described the key substantive offences under computer crime Act. Unauthorized access to a computer, any act to establish unauthorized access to commit a crime, operating a computer without legal authority, is an offence committed for national security and national economy and public order. It is also an offence to deal with illegal data and obtain data illegally, to interfere with data illegally, to use illegal equipment, and to unauthorized disclose of information that permits access to a service. There is a provision in the Act which enhances the scope of intellectual property provisions contained in the **Intellectual Property Act 36 of 2003**. An amendment made to the penal code in 2006 introduced an offence requiring all persons providing a computer service like a cyber cafe to ensure that such a service would not be used for offences relating to sexual abuse of a child. In addition, **Information Communication and Technology Act** and **Electronic Transaction Acts** are also specifically dealing with internet based crimes. Electronic Transaction Act facilitates to formation of contracts, the creation and exchange of data messages, electronic documents, electronic records. **Penal Code Amendment[[13]](#footnote-13)** and **Evidence (special provisions) Act** (No. 14 of 1995) is also used to prevent these crimes. According to Penal Code Amendment 286(b), it has a provision in “Duty of person providing service by computer to prevent sexual abuse of a child”. These things help to protect children from illegal internet uses. Evidence Act is also helpful to avert cyber-crimes.

**The legal framework of India**

**Practicality of cyber-crimes**

In February 2021—nearly one year from the start of the pandemic—there were 377.5 million brute-force attacks—a far cry from the 93.1 million witnessed at the beginning of 2020.With pandemic disrupting businesses and with remote working becoming reality, cyber criminals have been busy exploiting vulnerabilities. Year 2020 saw one of the largest numbers of data breaches and the numbers seem to be only rising.

According to Kaspersky’s telemetry, when the world went into lockdown in March 2020, the total number of brute force attacks against **Remote Desktop Protocol** (RDP)[[14]](#footnote-14) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase. The numbers in India went from 1.3 million in February 2020 to 3.3 million in March 2020. From April 2020 onward, monthly attacks never dipped below 300 million, and they reached a new high of 409 million attacks worldwide in November 2020. In July 2020, India recorded its highest number of attacks at 4.5 million.

*SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[[15]](#footnote-15)* is the first case of **cyber defamation** in India. On 17th August 2021 ‘The Times of India’ published a news about a cybercrime in Mumbai. In that case a 30 year old woman was duped of Rs. 2.4 lakh by a **cyber fraud** that posed as an army man and showed interest in buying her used furniture.[[16]](#footnote-16) In another case *State of Tamil Nadu v. Suhas Katti[[17]](#footnote-17)*, related to posting of obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced that the accused was in Mumbai and arrested him within the next few days. Relying on the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners, the Additional Chief Metropolitan Magistrate held the accused guilty of offences under Section 469, 509 of IPC and 67 of IT Act, 2000. Another important case *Shreya Singhal* Vs *UOI AIR[[18]](#footnote-18)* can be illustrated. In this case the two women were arrested under Section 66A of the IT Act, alleged to have posted objectionable comments on Facebook regarding the complete shutdown of Mumbai after the demise of a political leader. The women filed a petition challenging the constitutionality of Section 66A of the Act, alleging that it violated freedom of speech and expression. While pronouncing the decision the court held that section 66A is ambiguous, and is violation of the right to freedom of speech and it takes within its range the speech that is innocent as well. It removed an arbitrary provision from IT Act, 2000 and upheld citizens’ fundamental right to free speech in India.

One of the leading cybercrime cases is the **Bank NSP case[[19]](#footnote-19)** is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the bank’s computer to do this. The boy's company lost a large number of clients and took the bank to court.

In this way, the phenomenon has become a major theme in the world-famous Indian film industry as cyber crime is on the rise in India. As examples, movies like Vivegam (2017), Irumbu Thirai (2018),Kee (2019), Lens (2015) and Puriyatha Puthir (2017)etc. can be pointed out.

|  |  |
| --- | --- |
|  |  |

**Legal conditions**

 **The Information Technology Act**,[[20]](#footnote-20) 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime. The main objective of this Act is **to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes**.

There was a major need in the IT act to be amended and several major industries and corporates were consulted, contrast it with similar legislation of foreign nations and to recommend some suggestion for the development of this act. The suggestions were then scrutinize and then applied as effective Act. The main objective of ITAA are, Focusing on data privacy issues, Improving data security, Define cyber cafe, Neutralize the digital signature authority, Define intermediaries,

Recognizing the crucial role of Computer Emergency Role Team, Addition of offences like child pornography and cyber terrorism, Set legislation powers related to cyber-crime, Define different offences of cyber-crime like phishing, trojan horse, virus mails etc.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not “legal” in India. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in India have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

**In Information Technology Act,**

Section **65**- Whoever intentionally or knowingly destroys, conceal or change any computer’s source code that is used for a computer, computer program, and computer system or computer network, it is a tampering with computer source documents.

Section **66**- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, it is a hacking

Section **66A**- Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will, is the crime of sending offensive messages through communication services and it is punishable.

Section **66B**- Receiving or retaining any stolen computer, computer’s resources or any communication devices knowingly or having the reason to believe the same.

Section **66C**- Identify Theft Using of one’s digital or electronic signature or one’s password or any other unique identification of any person is a crime.

Section **66D**- Whoever tries to cheats someone by personating through any communication devices or computer’s resources shall be sentenced either with a description for a term that may extend up to 3 years of imprisonment along with a fine that may extend up to rupee 1 lakh. That is the crime of identity theft.

Section **66E**- Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

Section **66F**- Cyber terrorism

**A**. Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people by,

I. Deny to any people to access computer’s resources.

II. Attempting to break in or access a computer resource without any authorization or to exceed authorized access.

III. Introducing any computer’s contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavorably affect the critical information’s infrastructure specified under the section **70** of the IT Act.

**B**. By intention or by knowingly tries to go through or tries to gain access to computer’s resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer’s database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer’s database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of India.

Section **67**- whoever transmits or publishes or cause to publish any obscene materials in electronics form, Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend up to five years of imprisonment along with a fine which may extend up to 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend up to ten years along with a fine that may perhaps extend to two lakhs rupees.

Section **67A**- Whoever transmits or publishes materials that contains sexually explicit contents or acts shall be sentences for either description for a term which may extend up to 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees in the first convict. And in the event of the second convict criminal could be sentenced for either description for a term that could extend up to 7 years of imprisonment along with a fine that may extend up to 20 lakhs rupees.

Section **67B**- Whoever transmits or publishes any materials that depict **children** in sexually explicit act or conduct in any electronics form shall be sentenced for either description for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees 10 lakhs on the first conviction. And in the event of second conviction criminals could be sentenced for either description for a term that could extend to 7 years along with a fine that could extend to rupees 10 lakhs.

Section **67C**- Retention and preservation of information by intermediaries

I. Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the Central Government may prescribe.

II. Any intermediaries knowingly or intentionally contravene the provision of the sub-section.

Section **69**- Power to issue direction for monitor, decryption or interception of any information through computer’s resources

I. Where the Central government’s or State government’s authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of India, state’s security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section (II), for reasons to be recorded writing, direct any agency of the appropriate government, by order, decrypt or monitor or cause to be intercept any information that is generated or received or transmitted or is stored in any computer’s resources.

II. The safeguard and the procedure that is subjected to such decryption, monitoring or interception may have carried out, shall be such as may be prescribed.

III. The intermediaries, the subscribers or any individual who is in the charge of the computer’s resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access or access to computer’s resources receiving, transmitting, generating or to store such information or

b) Decrypting, intercepting or monitoring the information, as the case might be or

c) Providing information that is stored in computer.

IV. The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section

(III), shall be sentenced for a term that could extend to 7 years of imprisonment and also could be legally.

There are many other sections in the IT Act of India to prevent from cybercrimes. But these are the main areas of focus.

**Conclusion with suggestions**

Over the years, studies on cybercrime have shown a steady increase in the percentage of cybercrime that has occurred each year. With the advancement of technology and globalization, the circulation of social media and electronic devices has increased rapidly even among the ignorant community. Also, the less awareness of the people, the existing social and economic difficulties in accessing legal avenues, the unnecessary publicity given to the victims through the media, the unnecessary fear of legal access and the mental confusion etc. are the reasons for these crimes.

After analyzed the selected cases and challenges, such proposals are made to minimize the aforesaid criminal situations.

* Awareness about new media literacy (especially in all languages in Sri Lanka and India).
* Reform defamation laws and introduce cyber defamation laws.
* Introduce personal data protection Act.
* Introduce internet safe guard methods (especially for the parents and children).
* Creatively educate people to avoid cybercrime through social media.
* Increasing the tendency of victims to lodge complaints through the media without giving undue prominence to cyber-crimes.
* Developing the attitudes of the community including children, to make effective use of social media.

The enforcement of legal conditions and society in cyberspace, as suggested by researchers, will inevitably lead to a favorable trend in technological advancement. In Sri Lanka and India, as two adjacent countries in South Asia, when cyber-crime is quantitatively reduced, many positive conditions such as economic development and social security are established in the countries.

**Bibliography**

**Acts**

* Intellectual Property Act No.36 of 2003
* Sri Lanka Computer Crimes Act No. 24 of 2007
* The Computer Crime Act- 1997
* The Electronic Transactions Act No. 19 of 2006
* The Evidence (Special Provisions) Act No. 14 of 1995
* The Information and Communication Technology Act No. 27 of 2003
* The Information Technology Act- 2000 (India)
* The Payment and Settlement Systems Act No. 28 of 2005
* The Payment Devices Frauds Act No. 30 of 2006

 **Conventions**

* The convention on cybercrime (Budapest Convention) 2004 <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

 **Case Laws**

* *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*CM APPL No. 33474
* *State of Tamil Nadu v. Suhas Katti*
* *Shreya Singhal Vs UOI AIR*2015 SC 1523

**Articles**

* Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, ‘*A Brief Study on Cyber Crime and Cyber Law’s of* *India*’, Assam Kaziranga University
* Rahul Perukanda, ‘*Crimes in Cyberspace: Social Impact and the Legal Framework’*

 **Websites**

* (timesofindia.com) <https://m.timesofindia.com/topic/cyber-crime-cases>
* (coe.int) <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
* (infosecawaereness.in) <https://www.infosecawareness.in/cyber-laws-of-india>
* ( colombotelegraph.com) <https://www.colombotelegraph.com/index.php/cyber-security-an-analysis-on-awareness-on-cyber-security-among-youth-in-sri-lanka/>
* (rm.coe.int) <https://rm.coe.int/16802f264b>
* (meity.gov.in) <https://www.meity.gov.in/content/cyber-laws>
* (mondaq.com) <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>
* (mondaq.com) <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>
* (mondaq.com) [https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existencehttps://www.infosecawareness.in/cyber-laws-of-india](https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existencehttps%3A/www.infosecawareness.in/cyber-laws-of-india)
* (myadvo.in) <https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/>
* (irjet.net) [www.irjet.net](http://www.irjet.net/)
1. Rahul Perukanda, ‘*Crimes in Cyberspace: Social Impact and the Legal Framework’*, (Graduate , Law College - Sri Lanka ) 2020. [↑](#footnote-ref-1)
2. The convention on cybercrime (Budapest Convention), 2004. [↑](#footnote-ref-2)
3. Charindra, ‘*Cyber Crime in Sri Lanka Double in 2020’*,(11 September 2020) <https://www.themorning.lk/cybercrimes-in-sri-lanka-double-in-2020/>. [↑](#footnote-ref-3)
4. CISOMAG, ‘Sveral Websites in Sri Lanka Attacked’(20 May 2019) <https://cisomag.eccouncil.org/several-websites-in-sri-lanka-attacked/>. [↑](#footnote-ref-4)
5. Charindra, ‘*Cyber Crime in Sri Lanka Double in 2020’*,(11 September 2020) <https://www.themorning.lk/cybercrimes-in-sri-lanka-double-in-2020/>. [↑](#footnote-ref-5)
6. The Evidence (Special Provisions) Act, No. 14 of 1995. [↑](#footnote-ref-6)
7. The Information and Communication Technology Act, No. 27 of 2003. [↑](#footnote-ref-7)
8. The Payment and Settlement Systems Act, No. 28 of 2005. [↑](#footnote-ref-8)
9. The Electronic Transactions Act, No. 19 of 2006. [↑](#footnote-ref-9)
10. The Payment Devices Frauds Act, No. 30 of 2006. [↑](#footnote-ref-10)
11. The Computer Crime Act, 1997. [↑](#footnote-ref-11)
12. ‘*Cyber Care App Launched to Combat Cyber Violence in Sri Lanka’*(25 February 2021) <https://www.lk.undp.org/content/srilanka/en/home/presscenter/pressreleases/2021/Cyber_Care_App_launched_to_combat_cyber_violence_in_Sri_Lanka.html>. [↑](#footnote-ref-12)
13. Penal Code Amendment, No. 22 of 1995. [↑](#footnote-ref-13)
14. RDH,<https://www.thinstuff.com/products/rdh/?gclid=Cj0KCQjwvaeJBhCvARIsABgTDM5C1yLHUZn29yiFYX72RGcrzzchq5NsbJm4KoVH-vlfvUgHTd8CrW0aAsitEALw_wcB>. [↑](#footnote-ref-14)
15. *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra* CN APPl No. 33474. [↑](#footnote-ref-15)
16. ‘*Cyber Crime Cases’*(28 August, 2021) [https://m.timesofindia.com/topic/cyber-crime-cases](https://m.timesofindia.com/topic/cyber-crime-cases%22%20%5Ct%20%22_blank). [↑](#footnote-ref-16)
17. *State of Tamil Nadu v. Suhas Katti* CC No. 4680 of 2004. [↑](#footnote-ref-17)
18. *Shreya Singhal* *v*. *UOI AIR* 2015 SC 1523. [↑](#footnote-ref-18)
19. Shreya Taneja, ‘*Landmark Judgments on CyberLaw’* (01 June, 2021) <https://www.lawyersclubindia.com/articles/landmark-judgments-on-cyber-law-14025.asp>. [↑](#footnote-ref-19)
20. The Information Technology Act, No.21 of 2000. [↑](#footnote-ref-20)